édition 2008

LE DIRIGEANT DE PME-PMI & L'INTELLIGENCE ÉCONOMIQUE

Les précautions d'usage dans l'activité de la PME/PMI

CGPME Ile-de-France

AGEFOS PME ILE-DE-FRANCE

îledeFrance

« Le dirigeant de PME-PMI et l'intelligence économique »,

les précautions d'usage dans l'activité de la PME/PMI

1

CGPME
Ile-de-France®

© CGPME
Confédération Générale des PME,
Réalisation et conception technique par la CGPME Ile-de-France
EDITION 2008

2

Le Code de la propriété intellectuelle n'autorisant, aux termes des alinéas 2 et 3 de l'article L .122-5, d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analystes et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou production intégrale, ou partielle, faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause, est illicite » (alinéa 1er de l'article L.122-4).
Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles L. 335-2 et L. 335-3 du Code de la propriété intellectuelle.

La version actualisée en 2008 du guide « Le dirigeant de PME-PMI et l'Intelligence économique. Les précautions d'usage dans l'activité de la PME/PMI » fait l'objet d'un partenariat et d'un cofinancement entre :

CGPME IDF

Le Conseil Régional IDF

Agefos PME IDF

Avec nos remerciements pour l'appui du Commandement de la Région de Gendarmerie Ile-de-France, partenaire du programme d'action Intelligence Economique Stratégique en faveur des PME franciliennes.

Sommaire

L'Edito du Président de la CGPME Ile-de-France 6
L'édito des Président et Vice Président
du Conseil Régional d'Ile-de-France 7
L'édito des Présidents paritaires d'Agefos PME Ile-de-France 8
Introduction 9

1) Accompagner les mutations de la PME/PMI 16
A) L'Intelligence économique entre dans l'entreprise 16
B) Développer le travail en équipe En PME 23

2) Protéger ses infrastructures et le personnel 35
A) Securiser les locaux 35
B) Bien connaître son personnel 44

3) Maîtriser et sécuriser le pôle informatique 52
A) Un outil potentiellement vulnérable 52
B) Assurer la veille informatique 63

4) Gérer l'information et la communication 67
A) Organiser et protéger l'information 68
B) Emploi du temps, PDA et téléphonie mobile : les limites 73
C) Maîtriser ses contacts avec l'extérieur 78

Conclusion 88
Lexique 90
Annexes 97
Orientations bibliographiques 102
Sources électroniques d'information 105
Coordonnées utiles 106

L'Edito du Président de la CGPME Ile-de-France

Ce guide s'inscrit dans un contexte d'accroissement des tensions dans les relations économiques internationales. Il participe aux réponses impulsées au niveau régional par la CGPME Ile-de-France, dans le cadre du Schéma de Développement Economique Régional. Nous avons souhaité mettre l'accent sur les enjeux des mutations économique en Ile-de-France et les risques accrus de vulnérabilité des PME. Il leur est plus difficile aujourd'hui de préserver un avantage compétitif. C'est pourquoi la CGPME Ile-de-France, avec ses partenaires, le Conseil Régional Ile-de-France et Agefos PME Ile-de-France, jugent essentiel de faciliter l'accès des PME–PMI à l'intelligence économique et ses applications au sein de l'entreprise. Une nouvelle version du guide a été actualisée, afin de coller au plus près du contexte régional.

Nous vous proposons un guide pratique. Il ne s'agit pas de basculer dans une étude excessivement technique sur la notion d'intelligence économique. Nous avons décidé de nous adresser directement aux dirigeants qui, au sein des PME et PMI, sont en prise directe avec la réalité de la vie économique et commerciale, de plus en plus intégrée dans un marché non plus seulement régional ou national, mais international.

Pour gagner en clarté, nous nous appuyons sur des cas de figure pratiques, strictement fictifs, accompagnés de conseils pratiques, afin de pouvoir démultiplier facilement les informations au sein d'une entreprise. Pour faciliter cette accessibilité, nous accompagnons la réédition actualisée de l'ouvrage d'une parution bimestrielle de newsletters thématiques et opérationnelles à destination des pme franciliennes.

Nous mettons également en œuvre des réunions de sensibilisation et de formation pour nos partenaires territoriaux en Ile-de-France.

Il s'agit de créer ainsi les lieux de relais et de ressources au service des salariés et des dirigeants des PME-PMI sur les notions d'intelligence économique dans un contexte de concurrence de plus en plus vive, loin parfois des notions même d'équité, d'éthique et de respect de l'Autre. Nous souhaitons attirer l'attention sur les risques de dérive et les menaces qu'elles font peser sur les PME-PMI éprises de transparence et d'intégrité.

Jean-François ROUBAUD,

Président de la CGPME Ile-de-France.

L'édito des Président et Vice Président du Conseil Régional d'Ile-de-France

Dans un environnement toujours plus incertain et mouvant, la capacité pour les entreprises à se saisir des opportunités de marché devient un élément clé de leur compétitivité. Les PME-PMI, véritable poumon économique de l'Ile-de-France, sont particulièrement concernées par cette nouvelle donne. Ces entreprises, à l'origine des principales percées scientifiques, technologiques et commerciales, constituent le creuset de la création d'emplois. En leur apportant une vision plus affûtée de leur marché et de la concurrence, l'intelligence économique représente un atout fondamental pour leur développement.

Ce guide édité par la CGPME s'inscrit parfaitement dans la démarche du Schéma Régional de Développement Economique du Conseil Régional visant à promouvoir l'attractivité et la compétitivité des entreprises d'Ile-de-France. C'est un outil concret, pédagogique et pragmatique, qui entend faire, de l'intelligence économique, une réalité au sein des PME-PMI. Pour cela, bien plus que des recettes ou des techniques, il cherche à faire partager un nouvel état d'esprit. La rudesse de la compétition économique, loin de pousser au repli, nécessite au contraire, d'adopter des stratégies de développement encore plus offensives.

L'intelligence économique demande audace et inventivité. De plus, en reposant sur la nécessaire sensibilisation de tous les salariés de l'entreprise, elle contribue à replacer l'homme au cœur des enjeux, et donc l'économie au service du développement humain. Aujourd'hui plus que jamais, ce sont les femmes et les hommes de l'entreprise qui font la différence. Ils sont les clés de la réussite et donnent du sens au projet d'entreprise. C'est en cela, aussi, que l'intelligence économique s'inscrit dans les priorités des politiques conduites par la Région Ile-de-France.

Jean Paul HUCHON,

Président du Conseil Régional d'Ile-de-France.

Daniel BRUNEL,

Vice-président chargé de la formation professionnelle, du développement économique et de l'emploi.

L'édito des Présidents d'Agefos PME Ile-de-France

AGEFOS-PME Ile-de-France accompagne les PME franciliennes depuis plus de 30 ans dans leurs enjeux emploi / formation au quotidien. Dans un contexte incertain et instable, face aux nouveaux défis nés d'une concurrence internationale toujours plus dense, l'appropriation par les PME de bonnes pratiques de l'intelligence économique est une priorité à mettre en œuvre.

Elle est ainsi garante du développement des PME franciliennes et d'une démarche, reprise dans le présent guide, fondée sur l'appropriation et la formation de l'ensemble des salariés.

En Partenariat avec la CGPME Ile-de-France et le Conseil Régional Ile-de-France, l'AGEFOS PME Ile-de-France vous présente ce guide réactualisé sur les PME/PMI et l'Intelligence Economique. C'est avant tout un dispositif opérationnel qui vous permettra, de manière concrète et simple, d'appréhender cet enjeu clé, garant de la protection des PME dans leurs activités, le renforcement de leur démarche qualité et la réduction de leur vulnérabilité.

Présenté comme une chronique de la vie d'une PME au quotidien, ce guide est aussi un moyen de mettre en œuvre de nouvelles approches dans l'entreprise, en particulier dans le renforcement d'objectifs communs aux employeurs et aux salariés face aux risques et vulnérabilités qu'elle rencontre.

A l'instar de nos partenaires franciliens, nous faisons de l'intelligence économique une de nos priorités. Favoriser l'accès à ces nouveaux enjeux, permettre une appropriation opérationnelle de sa démarche, autant d'éléments au service de la pérennité des entreprises et de leurs salariés par l'acquisition de nouvelles compétences.

Les Présidents paritaires d'Agefos PME Ile-de-France.

Introduction,

Pourquoi ce guide ?

La CGPME est persuadée qu'il est aujourd'hui urgent de renforcer la sensibilisation des PME aux problèmes de l'intelligence économique. En effet, plusieurs facteurs convergent pour démontrer leur vulnérabilité, en matière de protection de l'information.

Un nouvel environnement économique

Tout repose essentiellement sur la prise en compte d'un nouvel environnement économique. L'économie de marché[1] est traversée par différentes logiques économiques, qui rendent la pratique de l'intelligence économique incontournable.

En marge des circuits économiques traditionnels, on remarque **les économies dites parallèles**, favorisant le développement et l'extension de commerces illicites : trafics d'être humaines, trafics d'armes et de drogues, et produits de contrefaçon. Et pour affiner l'industrie de la contrefaçon et sa diversification, il faut au préalable que les responsables puissent réunir des informations précieuses sur les produits de référence ; d'où leur recours à l'espionnage économique et à toutes les possibilités d'action que cela comporte.

On assiste surtout à **des conquêtes commerciales de plus en plus agressives.** L'ouverture des marchés a favorisé la multiplication des concurrents directs. Désireuses de ne pas perdre pied dans leur propre secteur, les entreprises délocalisent vers les pays où le prix de revient de la main d'œuvre est plus attractif.

La situation est particulièrement préoccupante dans **le domaine des secteurs dits stratégiques,** où les matières premières à haute valeur ajoutée, tels les produits énergétiques, la recherche liée aux nouvelles technologies, sont touchés de plein fouet par une vive concurrence. Si bien que la guerre économique vise essentiellement les secteurs des industries de Défense, des énergies, des transports et de l'aéronautique.

1) Issue d'Occident, elle s'est peu à peu forgée dès le Moyen-Âge pour devenir une source de puissance en particulier pour les Cités-Etats, puis les Etats-nations de l'époque moderne ; plus exactement entre les XV^{ème} et le XVIII^{ème} siècles.

La guerre économique est animée par ces logiques, avec un point commun : le rôle clé de l'information et de la désinformation…

Des PME au cœur de la guerre économique

Les petites et moyennes entreprises s'inscrivent dans la même logique : consolider leur assise, sur un marché de plus en plus éprouvant, en préservant leurs acquis et en se projetant si possible vers de nouveaux marchés. La dynamique de l'entreprise repose alors essentiellement sur ses capacités à obtenir des informations. Celles-ci sont en effet indispensables pour aiguiser une stratégie de développement adaptée aux contraintes du marché.

Une révolution technique

Au cœur des mutations économiques, interviennent les Nouvelles Technologies de l'Information et de la Communication (NTIC). Avec le réseau Internet, ce sont quelques six milliards de données qui deviennent accessibles. Pour ne pas basculer dans la surinformation, il faut savoir gérer, trier et classer les données collectées et en retirer l'essentiel. Le nouveau siècle qui s'ouvre à nous révèle à quel point les activités économiques reposent sur la communication virtuelle via Internet et les multiples réseaux intégrés. L'utilisation croissante de « moteurs de recherche » contribue à un recueil toujours plus rapide des informations, notions-clé dans la vie des PME-PMI. Une profusion de données en temps réel qui, pour être exploitées, exige rigueur et méthode pour ne pas être dépassé, écrasé par le volume. En même temps, il faut savoir être vigilant pour surveiller et analyser le jeu des concurrents.

Le rôle clé du chef d'entreprise

Le chef d'entreprise a évidemment un rôle-clé dans cette démarche. Il insuffle une véritable dynamique de précaution, de préservation des acquis. Il a aussi le devoir de protéger son entreprise et ses actifs. En cas de problème majeur, sa responsabilité civile et pénale peut d'ailleurs être engagée. A l'inverse, les salariés d'une entreprise doivent être considérés et – se considérer – comme des acteurs de premier plan de leur propre structure. L'esprit d'initiative, la démarche collective ont alors une forte résonance.

Ce qui nous amène, avant d'aller plus loin, à détailler la notion même d'intelligence économique.

Qu'est-ce que l'intelligence économique ?

Dans le prolongement de cette démarche méthodologique, l'information devient un enjeu de rivalités lorsqu'elle se fait rare ; elle peut peut-être devenir le moyen de lutte – dans un cadre de guerre par l'information – avec la perspective de conserver un avantage compétitif.

L'intelligence économique peut être définie comme la maîtrise autant que la protection – en clair la gestion – de l'information stratégique.

Ce qui revient à dire que l'intelligence économique réunit des savoir-faire qui s'organisent autour de trois axes :

- l'un repose sur des actions offensives-défensives (veille),
- l'autre sur la recherche des menaces et des sources d'informations opportunes (sécurité économique, sûreté protection du patrimoine informationnel).
- Le troisième, quant à lui, porte sur l'influence et le management des perceptions.

Elle interpelle le personnel des entreprises sur les conduites à tenir, les principes minimums de précaution qu'il faut remplir. Autant d'éléments sur lesquels nous allons revenir.

L'information stratégique intègre non seulement les données technologiques mais aussi la santé financière de l'entreprise, ses réseaux commerciaux, ses méthodes de production et de distribution.

La collecte des informations relevant de l'intelligence économique est parfaitement légale puisque 90% de ces informations sont libres d'accès, via notamment les salons, les colloques. Restent 10% d'informations qui peuvent être obtenus par le jeu du renseignement. Ce dernier est assuré soit directement par les entreprises elles-mêmes, soit par des sociétés de renseignement privées. En soit, il s'agit d'obtenir des informations difficiles d'accès, de manière plus ou moins légale. Les méthodes, délicates, nécessitent parfois plus de temps pour pouvoir accéder aux informations visées. Certains, pour obtenir les éléments recherchés, n'hésitent pas à commettre des vols de documents, à acheter frauduleusement des informations, à s'appliquer au jeu de la corruption.

Toute la démarche se focalise en fait sur des questions essentielles : comment reconnaître la bonne information ? Comment disposer de cette information ? Toute la difficulté est là.

Lorsque l'on parle de renseignement dans le secteur privé, on trouve alors les notions d'interception, de piratage et de manipulation ; ce qui ne peut

aboutir, à terme, qu'à une révolution des mentalités et une réelle sensibilisation aux notions de prévention/défense et attaque.

L'économie repose désormais sur un maillage de réseaux plus ou moins opposés, au centre desquels la connaissance est à la fois source d'émulation (dynamisme de l'entreprise) et de convoitise (concurrence des entreprises).

Les grandes entreprises françaises, essentiellement dans les secteurs aéronautique, énergétique, pharmaceutique et industrialo militaire sont désormais bien loties et capables de faire face.

Dès lors, l'attention de la Confédération Générale des PME, se porte aujourd'hui sur les PME/PMI qu'il faut sensibiliser à la création d'un pôle d'intelligence économique en leur sein. Elle rejoint en cela les initiatives régionales et gouvernementales, se traduisant par l'action simultanée du Conseil Régional d'Ile-de-France, du ministère de l'Intérieur, de l'Agence pour la diffusion de l'information technologique (Adit), des Agences régionales d'information stratégique et technologique (Arist), de l'association française pour le développement de l'intelligence économique (Afdie).

De manière assez concise, on retiendra que l'intelligence économique intègre donc des savoir-faire transdisciplinaires : veille, sécurité économique et influence.

En bref... « Points clés formation »

L'intelligence économique est la somme de tous les moyens destinés à préserver les informations vitales pour l'entreprise. Afin d'éviter qu'un concurrent s'en empare pour les réutiliser à son profit.

Il est important de souligner que l'intelligence économique ne peut être réduite au seul espionnage industriel lorsque sont abordées les questions de renseignement et de concurrence déloyale.

Le rôle du chef d'entreprise :

- Maîtriser et protéger l'information de son entreprise ;
- Utiliser les moyens informatiques de veille, d'analyse et de protection ;
- Mener des recherches et avoir une démarche de prospective ;

Les fondements de l'intelligence économique (IE) :
- Gestion et protection de l'information et des connaissances ;
- Influence et contre-influence dans le but de finaliser la compétitivité ;
- Sécuriser la vie économique de l'entreprise et consolider l'influence du pays (patriotisme économique).

Mode d'emploi du guide

Illustrations de problèmes concrêts...

L'essentiel de notre étude porte sur **le suivi, pendant un mois environ, d'une société fictive** – insistons sur ce point – spécialisée dans la production et la distribution de ventilateurs. Une entreprise de 20 employés qui aspire à diversifier ses marchés, à s'étendre à l'international. A travers ce cas concret, nous ferons le point sur les défis majeurs et les menaces qui se présentent au personnel de l'entreprise.

A noter d'ailleurs que l'accumulation des difficultés mises en lumière dans le présent ouvrage est fortement improbable en un laps de temps aussi réduit. Il faut donc les prendre en compte avec le recul nécessaire ; le but étant simplement d'illustrer le propos.

A maintes reprises, nous insisterons sur un impératif : la qualité des relations humaines, fondée sur une solide communication interne.

Le repère de quatre semaines permettra de mettre l'accent sur une trentaine de points essentiels, au gré des thématiques suivantes : environnement physique et humain ; domaine informatique ; communication, information ; services externes. De là découleront une série de conseils, de principes méthodologiques qui peuvent être appliqués pour assurer une bonne protection de l'entreprise sur un marché tant national qu'international, inscrit dans une logique de concurrence effrénée.

... synthétisées par les points clefs formation

Pour que ce guide constitue un outil de formation efficace, chaque partie est résumée dans des Points Clefs Formation, qui rassemblent les bonnes pratiques à adopter en matière d'intelligence économique. Ils regroupent l'essentiel des informations pouvant être transmises au sein de l'entreprise. Ainsi, avec ce guide, le dirigeant dispose autant d'un outil d'autoformation que de formation de ses salariés.

Carte d'identité de l'entreprise *Ventili*

(Toute ressemblance avec une société de même nom déjà existante est bien entendu fortuite)

Domaine d'activité : conception et vente de ventilateurs
Nombre de salariés : 20
Localisation : Issy-les-Moulineaux (proche banlieue parisienne)
Sous-traitants : pour la commercialisation des produits de *Ventili*
Logique commerciale : exportation
Marché : national et international

Les personnages-clés de *Ventili*

- Pierre Darmond, directeur de *Ventili* ;
Homme d'affaires avisé, disposant d'une solide expérience professionnelle, il fait preuve d'un fort esprit d'initiative et d'une capacité d'adaptation naturelle. Vif, curieux, il apprécie le travail d'équipe et base le fonctionnement de son entreprise sur des principes de transparence et de respect mutuel avec l'ensemble du personnel. Pour lui , la Femme, l'Homme, les actifs sont les garants de l'efficacité de l'entreprise.

- Michèle Attenet, responsable des Ressources humaines ;
Diplômée de sociologie, elle a suivi un cursus complémentaire en Gestion des Ressources humaines dans l'enseignement supérieur privé. Elle fut enseignante de sociologie avant de se consacrer pleinement à la vie d'entreprise.

- David Brissard, directeur du Service informatique ;
Ingénieur de formation, il est passionné par sa spécialité informatique et a travaillé dans une importante multinationale de production informatique avant d'opter pour le monde plus intimiste d'une PME.

- Annie Baral, responsable de la Communication ;
Diplômée d'une Ecole de Communication, elle a notamment été journaliste quelques années dans la presse avant d'être séduite par une implication professionnelle dans le milieu des PME-PMI.

- **Alain Pautrat,** responsable de la Gestion de production ;

A suivi un cursus interdisciplinaire tout en occupant successivement divers postes à responsabilité dans le secteur industriel. Spécialiste de métallurgie et ami de Pierre Darmond dont il partage la conception de la vie entrepreneuriale, il a décidé de mettre son savoir-faire au profit de Ventili.

- **Françoise Chenay,** pour le département Recherche ;

Ingénieur, spécialiste de la chimie des matériaux, et d'aéraulique, il fut Chargé de cours à l'Université pendant ses années de Doctorat. Puis, préférant le milieu plus concret de l'entreprise, il a été recruté par Pierre Darmond.

- **Georges Messonot,** pour le Service commercial ;

Initialement autodidacte, G. Messonot s'est peu à peu spécialisé dans le secteur de la ventilation, avec expérience professionnelle de 25 ans ; d'abord pour un gros producteur français avant de rejoindre Ventili.

Enfin, le dernier venu dans l'entreprise *Ventili* :

- **Eric Chatran,** spécialiste d'intelligence économique, chargé de mission ;

Diplômé d'Ecole de Commerce, il a travaillé comme chargé de mission pour le ministère de la Défense puis le Ministère de l'Économie, des Finances et de l'Industrie (MINEFI) en tant que collaborateur dans l'application des stratégies d'implantation d'entreprise française à l'étranger et les pays d'accueil. Puis il s'est tourné vers la protection des données stratégiques des entreprises françaises publiques à l'international.

1) Accompagner les mutations de la PME/PMI

L'intelligence économique est donc essentielle à la bonne marche des activités d'une entreprise. Insistons à présent sur les secteurs-clés pour une entreprise en conciliant approche théorique et exemple pratique, en nous référant à une société fictive.

A) L'intelligence économique entre dans l'entreprise

Avant tout, cernons la démarche de la direction de *Ventili*, au travers d'une rapide synthèse concernant la création puis la montée en puissance de la société.

Savoir être compétitif

Pierre Darmond, directeur de *Ventili*, a une longue expérience professionnelle dans le domaine commercial. Il a occupé divers postes de gestionnaire et de responsable dans des pôles de direction de plusieurs grandes entreprises pendant près d'une vingtaine d'années. Puis, après une étude de marché et maintes réflexions, il s'est lancé et a créé sa propre entreprise. Tenant compte des enseignements tirés au gré de son parcours personnel, il a évité bien des écueils et forgé pendant une dizaine d'année son entreprise. Celle-ci bénéficie désormais d'un potentiel confortable. Elle jouit d'une parfaite crédibilité sur le marché national.

Initialement, Pierre Darmond s'est focalisé sur un marché national destiné aux professionnels. Puis, grâce à la qualité de ses produits, servi par ses pôles de distribution, il a peu à peu étendu son marché auprès des consommateurs

en général. En même temps, il a su diversifier ses produits et proposer plusieurs gammes. Satisfait des résultats, il souhaite désormais s'implanter sur le marché international.

En quelques années, *Ventili* s'est hissé parmi les entreprises nationales les plus en pointe dans le secteur de la ventilation. Conjointement, la direction a renforcé progressivement ses équipes tant au niveau de la production que de la commercialisation/distribution et, enfin, de la communication. Et en permanence, le directeur n'a eu de cesse de fortifier un véritable esprit d'entreprise, un esprit de groupe sinon de corps. Pierre Darmond est convaincu que la réussite de son activité repose avant tout sur la qualité des relations humaines au sein de son entreprise, alors que la concurrence se montre de plus en plus rude et déloyale.

« Points Clefs Formation »

Quelques principes basiques

Pour être efficace et durable, l'entreprise doit se montrer compétitive en sachant produire et vendre. Elle doit être innovante pour proposer des produits de différentes gammes et d'une qualité toujours préservée voire améliorée, qui tiennent compte des attentes des consommateurs, de l'évolution du marché qui la concerne. En même temps, elle doit favoriser, en interne, l'émergence de nouvelles méthodes, pour un bon dynamisme collectif et une étroite collaboration.

Cela va de pair avec une attention particulière portée à la qualité des relations interservices, à la bonne ambiance dans l'entreprise. Un vecteur porteur pour assurer à la fois dynamisme et productivité des employés, sereins et satisfaits de travailler dans de bonnes conditions. Or, ces principes – pourtant élémentaires – font trop souvent défaut.

Fédérateur, meneur d'hommes, Pierre Darrmond s'est entouré d'une équipe de direction à la fois dynamique et en parfaite harmonie avec sa conception de la vie et de la primauté donnée aux valeurs humaines. Est ainsi mise en avant la notion de transparence relationnelle. Les moindres tensions ou incompréhensions sont naturellement mises à plat, au cours de discussions et négociations tenues sereinement. Ainsi, les différends ont-ils toujours pu être gérés. Cette politique du compromis et de la transparence a fini par devenir une culture d'entreprise, à contre-courant de la tendance générale. En effet,

dans nombre de PME-PMI, les activités pâtissent de conditions et ambiances de travail déplorables. De cette manière, la méthode de Pierre Darmond rend son entreprise particulièrement attractive et dynamique.

A présent, Pierre Darmond met en avant les mesures de protection non seulement du savoir-faire de la production, mais aussi des infrastructures. A cela s'ajoute sa volonté de protéger les employés contre les pressions extérieures, et d'éviter toute fuite d'informations.

Il a su s'entourer de collaborateurs tous aussi attentifs à cet aspect de protection/préservation de l'entreprise : Michèle Attenet, responsable des Ressources humaines, David Brissard, directeur du Service informatique, Annie Baral, responsable de la Communication et Alain Pautrat, responsable de la Gestion de production, Françoise Chenay, pour le département Recherche, et Georges Messonot pour le Service commercial. On l'a vu, tous ont acquis au préalable une expérience professionnelle significative. Au fur et à mesure, ils se sont sensibilisés aux questions d'intelligence économique, au gré de colloques organisés, ces derniers mois, par le Ministère de l'Economie des Finances et de l'Emploi, en collaboration avec la Fédération des professionnels de l''intelligence économique (FéPIE). Au sein de *Ventili*, après plusieurs réunions de concertation avec Pierre Darmond, tous ont accepté de privilégier la protection interne et externe de *Ventili*. En clair, ils sont devenus attentifs aux questions d'intelligence économique.

La protection interne et externe…

Ainsi, pour la direction collégiale de *Ventili*, il s'agit d'assurer la protection des infrastructures et du personnel ; de même que la protection des pôles décisionnels et des informations qui en émanent.

En second lieu, il s'agit aussi de disposer d'un potentiel de recueil de l'information. Cela nécessite la mise en place d'un service de veille informatique, destiné à gérer l'information. Car, faut-il le rappeler, les nouvelles technologies facilitent la diffusion des informations, fausses ou véridiques, importantes ou dérisoires.

Pierre Darmond, le directeur de *Ventili*, décide alors de contacter quelques proches qui œuvrent à leur compte dans l'intelligence économique (IE). En même temps, il s'interroge sur la forme du service envisagé. Doit-il faire appel à un sous-traitant spécialisé dans l'intelligence économique ou, au contraire, constituer son propre pôle d'intelligence économique au sein même de son entreprise ? Finalement, en tenant compte des divers conseils qui lui sont prodigués, il décide de monter lui-même un service d'IE au sein de *Ventili*. Son choix définitif tient compte aussi des capacités budgétaires de l'entreprise,

capables de supporter un tel renforcement de ses moyens et dépenses en la matière.

« Points Clefs Formation »

Penser au pôle de veille informatique

Les PME, en fonction évidemment de leurs capacités financières et de leur stratégie commerciale, peuvent donc se doter d'un pôle de veille relié à l'Internet, avec un prolongement attentif à ce qui se crée, s'écrit dans leur secteur d'activité ; non pas seulement sur le plan national mais aussi au niveau international.

Pierre Darmond décide alors de recruter un chargé de mission expérimenté en sécurisation d'entreprise, disposant d'une formation juridique et fin connaisseur de toutes les dimensions de l'intelligence économique. Il recherche un homme, à la fois de tête et de terrain, capable de manager une équipe plurifonctionnelle. Les candidatures affluent. Car, en tant que telle, l'intelligence économique constitue un marché porteur.

Au terme d'une série d'entretiens, le directeur en concertation avec Michèle Attenet, choisit un actif d'une quarantaine d'année, Eric Chatran, désireux d'agir dans le secteur privé après une longue expérience dans le secteur public. Eric Chatran est séduit par le dynamisme de *Ventili*.

Dès le début de sa mission, Eric Chatran, s'attache à sensibiliser les employés de *Ventili* aux principes de l'intelligence économique dans l'entreprise. A ce titre, il organise plusieurs séances d'information à leur intention. A raison d'une heure hebdomadaire, en fin de matinée, pendant trois semaines consécutives, la direction tient une réunion plénière où le Directeur, Pierre Darmond, et Eric Chatran prennent la parole pour mettre l'accent sur l'importance de la logique de précaution. Notion d'autant plus importante que *Ventili* se tourne vers l'international pour conquérir de nouvelles parts de marché.

Eric Chatran en profite notamment pour insister sur la dureté du marché international en termes de concurrence. Il souligne le caractère offensif – sinon agressif – des concurrents. Au début, l'assemblée n'était guère portée sur les

questions d'intelligence économique. Certains jugeaient cela dérisoire, relevant de la fantasmagorie et du délire sécuritaire. Mais, au fur et à mesure, les employés de l'entreprise prirent la mesure des enjeux et défis qui se présentent à eux. Ils ont réalisé combien ils avaient eu des préjugés et qu'au final, les impératifs de sécurité économique étaient essentiels.

…dans un contexte de concurrence

Les employés de *Ventili* sont bien conscients de l'affirmation d'une forte concurrence, de dimension internationale, en provenance de l'Asie. Si l'offensive japonaise a surtout été palpable à la fin des années 1980, c'est désormais l'offensive de l'économie chinoise qui est au cœur de toutes les analyses et de toutes les appréhensions.

« Points Clefs Formation »

Face à l'adversité

Cela oblige à une nécessaire réaction de *Ventili*. sachant que, contrairement à ce que l'on pourrait croire, les Chinois ne se focalisent pas sur la seule production bon marché. Ils ne sont pas seulement capables de produire des ventilateurs bon marché par exemple. Désormais, ils privilégient la production de qualité, voire même de haute qualité, en s'imprégnant des savoir-faire des produits occidentaux, français en particulier.

La direction de *Ventili* sait que l'affrontement concurrentiel entre les principaux constructeurs de ventilateurs du monde, va devenir particulièrement rude au regard des mutations climatiques (réchauffement de l'atmosphère et hausse des températures moyennes).

« Points Clefs Formation »

Privilégier la qualité

Devant les exigences des consommateurs, tout repose sur la qualité des produits, gage de crédibilité et donc de meilleure compétitivité. Ce qui montre, de toute évidence, que l'on peut être aussi bien placé sur l'échiquier international en proposant des produits de qualité, y compris dans des secteurs qui, jusqu'alors, n'y étaient pas foncièrement habitués. Le bon sens populaire n'a-t-il pas retenu qu'en fin de compte, « le bon marché coûte cher » ?

Tous ces aspects sont largement pris en compte par l'équipe de direction de *Ventili*. Et le service de communication interne de l'entreprise insiste régulièrement sur ces points, dans le courrier hebdomadaire interne.

Conjointement, Pierre Darmond met l'accent sur la centralisation de toutes les informations portant sur l'évolution du marché. Il a pour cela sollicité les diverses composantes de l'entreprise.

La place essentielle du renseignement

La direction de *Ventili* insiste en effet pour que ses campagnes commerciales reposent sur les renseignements recueillis ; en s'imprégnant par exemple des attentes du public en matière de ventilation.

« Points Clefs Formation »

Répondre aux questions essentielles de la consommation

Quels sont les types de ventilateurs les plus en vogue ? Quelle est la meilleure fourchette de prix pour ne pas dissuader le client ? Ces divers éléments, loin d'être occasionnels ou ponctuels, doivent être réactualisés régulièrement en tenant compte du contexte social et économique. Au-delà de la seule santé des marchés boursiers dont les variations sont généralement artificielles et passionnelles.

Les informations recueillies par *Ventili* doivent aussi prendre en compte les risques que représentent les jeux d'influence, les éventuelles démarches de désinformation, ou de déstabilisation, de la part de ses puissants concurrents.

Chargé de dépouiller les informations, de les classer et de les exploiter, le service d'Eric Chatran, se pose des questions fondamentales : est-ce que les informations obtenues sont fiables ? Peut-on baser notre stratégie commerciale, notre démarche productive sur elles ?

Aussi Eric Chatran prend-il le soin de répéter sans cesse à ses deux collaborateurs que lui a délégués Pierre Darmond, de systématiquement recouper l'information, de la valider par plusieurs canaux de confiance : contacts humains, diverses sources sans lien direct. Eric Chatran, pour cela, fait jouer ses relations, fiables, qui œuvrent pour leur propre compte dans l'intelligence économique, sans aucun lien avec *Ventili*. Et cela sans qu'il y n'ait conflit d'intérêt.

En agissant de la sorte, l'entreprise de Pierre Darmond démontre sa vigilance face à toute menace susceptible d'atteindre son potentiel. Elle s'imprègne à tous les niveaux des nouvelles exigences du marché. *Ventili* a ainsi adopté, en quelques semaines, la logique de maîtrise indispensable des informations, bénéficiant en cela de l'ère de la médiatisation, grâce aux vecteurs des Nouvelles technologies de l'information et de la Communication (NTIC).

« Points Clefs Formation »

Un atout : La gestion stratégique de l'information économique

En permanence, *Ventili* doit s'adapter au contexte de concurrence effrénée des échanges. L'entreprise doit être capable d'accéder aux informations stratégiques pour mieux anticiper les marchés futurs et les actions des concurrents ; une démarche méthodologique qui peut être résumée par la notion de gestion stratégique de l'information économique.

A l'inverse, l'entreprise doit s'imprégner d'une conjoncture d'offensive dite généralisée. Elle ne peut donc plus se limiter à la seule compréhension et anticipation des stratégies de ses concurrents. Elle doit être en mesure de résister aux attaques auquel son propre système de communication, son réseau informatique (autrement dit son patrimoine informationnel), ses intérêts vitaux sont exposés.

Mais toute cette méthode ne peut exister sans le rôle-clé du facteur humain. Et Pierre Darmond en a été de plus en plus convaincu au gré de son parcours professionnel. C'est un impératif qu'il faut appliquer pour pouvoir, de là, pratiquer les méthodes d'intelligence économique.

B) Développer le travail en équipe en PME

Au préalable, tout repose donc sur le travail en équipe. Le directeur de *Ventili* est convaincu qu'il vaut mieux appliquer un principe participatif que directif dans sa propre structure. Une réelle coopération interservices, une sincère implication dans la vie de l'entreprise, la fluidité de communication entre les pôles organisationnels et au sein de chacun d'eux ; autant de qualités loin d'être observées de manière large, déplore Pierre Darmond, dans les entreprise aujourd'hui.

La conscience professionnelle, premier élément d'IE

Pierre Darmond n'a eu de cesse de le répéter au gré des réunions avec les divers chefs de service, conscient que la conjoncture est à la morosité, au malaise social et donc à l'essoufflement des motivations :

« Nous devons regonfler le moral de notre personnel, de nos équipes. Surtout à l'heure de l'émergence d'une forte concurrence en provenance des pays d'Asie du Sud-Est. Nous sommes dans une société où l'individualisme est trop répandu. Paradoxalement, c'est même devenu le modèle de référence en matière de fonctionnement social. Or dans une entreprise, où la réussite dépend de l'action collective, il est évidemment contraire au principe d'intérêt général. Le service de Communication interne doit notamment contribuer à ce que chaque employé – mais à condition qu'il se sente bien dans l'entreprise ! – puisse s'investir dans les objectifs communs. Mais, faut-il insister sur ce point, l'investissement de chacun ne doit pas être motivé par un paternalisme opportuniste de notre part. Etablissons des relations saines, basées sur la transparence, la confiance.

Ce n'est pas la pression psychologique qui doit être l'élément moteur pour dynamiser l'esprit collectif. Il faut éviter tout harcèlement moral qui engendre en réaction de plus en plus en procédures judiciaires de la part des personnes qui en sont victimes. Cela ne peut que nuire à l'entreprise, tant au niveau de son image de marque qu'en perte d'énergie, sans oublier le coût des répercussions judiciaires.

Si les relations sont artificielles, forcées ou sous influence, les employés s'appliqueront à une survie professionnelle. Ils prendront sur eux un temps pour préserver leur emploi. Mais ils ne seront pas pour autant motivés par la vie de l'entreprise et détesteront leur direction et ses représentants. »

« Points Clefs Formation »

Primauté des ressources humaines

Le chef d'entreprise et, de manière plus large, l'équipe directionnelle – quelle qu'en soit la forme et le volume – doivent façonner des liens entre les employés, entre les divers services pour créer une véritable dynamique de groupe.

Il est impératif de s'appliquer à des relations saines et sincères. En créant de véritables liens socio-professionnels, fondés sur le respect et la confiance, une solide capacité d'écoute non feinte et une démarche qui prône le dialogue régulier et des efforts pour désamorcer tout malentendu, la direction de l'entreprise s'inscrit alors dans une logique constructive

En favorisant l'investissement collectif dans la vie de l'entreprise, Pierre Darmond, contribue à la montée en puissance de *Ventili*. L'entreprise ne peut être viable que si le personnel s'y sent bien et se sent concerné par la productivité de l'entreprise elle-même.

Pierre Darmond martèle ainsi souvent son credo. Sa démarche consiste aussi à venir discuter chaque semaine avec ses employés, en passant dans les ateliers.

En témoignant d'un sincère esprit d'équipe, la direction de *Ventili* entretient ainsi l'émulation collective. Elle doit aussi pour cela savoir encourager, remercier, féliciter son personnel. Des signes de respect, de correction élémentaire, des témoignages de reconnaissance qui, en toute logique, motivent les employés, consolident le travail d'équipe et forgent un corps en mesure de faire face à l'adversité. La concurrence déloyale, via ses attaques plus ou moins directes – nous y reviendrons – est alors endiguée par une politique de sécurité dans l'entreprise. Pierre Darmond appelle de surcroît chacun des employés de l'entreprise à la vigilance, en particulier les assistantes et les secrétaires qui occupent des postes-clés entre les divers pôles de l'entreprise, et l'extérieur avec lequel elles sont en prises directes.

« Points Clefs Formation »

Préserver les compétences, perpétuer les savoir-faire

Au-delà du seul domaine de la veille informatique, trop d'entreprises sont victimes de leur manque d'anticipation, de prévision et de réorientation en matière de gestion des ressources humaines. On le voit ne serait-ce qu'au niveau des départs en retraite. Il faut assurer la transmission des savoir-faire, des compétences minimales pour conforter le suivi des dossiers, des secteurs-clés ; même si, en toute logique, on ne pourra attendre de la part des nouveaux venus, le même degré d'expérience des salariés en passe de quitter le monde actif.

Conscience professionnelle, responsabilité collective

La démarche collective – dont la dynamique dépasse la simple somme de responsabilités individuelles – est donc essentielle en matière d'intelligence économique. Aussi, l'ensemble du personnel doit-il être appelé à contribution et, en retour, recevoir des informations précises quant à l'état du marché, l'évolution de la tendance conjoncturelle, etc. En clair être régulièrement mis au courant de la situation de l'entreprise à tous les niveaux.

Les collaborateurs ne peuvent adhérer à la politique de sécurité mise en place qu'à condition d'y être sensibilisés par le biais notamment d'une charte d'utilisation. En dehors de l'intention frauduleuse, réduite de toute évidence, la formation/sensibilisation des salariés contribue à réduire les failles dans le système de sécurité. Car, ne l'oublions jamais, le facteur humain est au cœur des activités économiques. Il peut donc être porteur comme il peut être votre pire obstacle si vous ne faites pas preuve d'ouverture d'esprit et d'attention.

Utiliser la formation professionnelle continue

Préserver les informations vitales pour l'entreprise nécessite l'acquisition de compétences spécifiques individuelles et collectives, une capacité à clarifier les droits et les devoirs en matière de formation et surtout l'articulation entre la formation professionnelle, les enjeux de l'intelligence économique et l'évolution professionnelle du salarié.

La signature de l'Accord National Interprofessionnel le 20 septembre 2003 a permis la promulgation de la loi du 4 mai 2004 relative à la formation professionnelle tout au long de la vie.

Les nouveaux objectifs assignés à la formation professionnelle [2] continue tout au long de la vie sont clairs : permettre le maintien de l'emploi par l'adaptation des salariés au changements des techniques et à l'évolution de l'emploi, favoriser le développement des compétences et l'accès aux différents niveaux de qualification, contribuer au développement culturel, économique et à la promotion sociale.

La loi prend également en compte des avancées significatives dans plusieurs domaines, notamment :

- la création d'un droit individuel à la formation, mis en œuvre pour partie en dehors du temps de travail,
- la mise en place d'une période de professionnalisation pour les salariés
- l'accroissement des dispositifs financiers des entreprises et notamment des TPE / PME.

« Points Clefs Formation »

Le plan de formation de l'entreprise

Le chef d'entreprise doit préciser dans un document d'information la nature des actions proposées qui peuvent relever de trois catégories :

- des actions d'adaptation au poste de travail,
- des actions liées à l'évolution des emplois ou participant au maintien dans l'emploi,
- des actions de développement des compétences.

2) Voir également en annexe l'explication concernant le principe de gestion paritaire de la formation professionnelle.

Le droit individuel à la formation (DIF)

Le DIF permet au salarié de bénéficier d'actions de formation d'une durée minimale de 20 heures par an, cumulables sur 6 ans.

Les types de formation éligibles au DIF doivent relever, soit des actions de promotion, soit des actions d'acquisition, d'entretien ou de perfectionnement des connaissances, soit des actions de formation conduisant à l'acquisition de diplômes, d'un titre à finalité professionnelle ou d'une qualification reconnue par une convention collective.

La période de professionnalisation

L'objectif de ce contrat de formation en alternance est de permettre aux salariés en place d'acquérir un diplôme, un titre ou une qualification, notamment ceux dont la qualification est inadaptée à l'évolution des technologies et des organisations.

Le congé individuel de formation (CIF)

Le CIF donne la possibilité à un salarié d'obtenir un congé de formation et de bénéficier d'actions d'accompagnement et de conseil lui permettant de construire son projet professionnel et de rechercher les moyens les mieux adaptés pour le mettre en œuvre, en s'appuyant notamment sur le bilan de compétences et la validation des acquis de l'expérience (VAE) : obtenir un diplôme, changer de métier, se reconvertir, ou encore se prémunir face aux incertitudes du marché de l'emploi…

L'entretien professionnel

Cet entretien est obligatoire pour toutes les entreprises et tous les 2 ans. Il est donc nécessaire d'informer et de former le personnel d'encadrement concernant les dispositions de la loi sur la formation professionnelle, afin de pouvoir informer les salariés de leurs droits relatifs aux dispositifs liés aux compétences : DIF, CIF, VAE, bilan de compétences, période de professionnalisation…

La notion de gestion collective face aux menaces

Au regard de la concurrence des entreprises chinoises, Eric Chatran oriente sa collecte d'informations sur la réalité de leur potentiel en matière de commercialisation de ventilateurs. Il s'applique aussi recueillir des informations sur les caractéristiques techniques desdits ventilateurs. D'où la nécessité d'une gestion collective de l'information (entre collecte, traitement et redistribution vers des alliés).

Pierre Darmond y est très attaché, sachant que le traitement des sources ouvertes n'est évidemment pas problématique. L'accent doit être mis sur la préservation des moyens d'informations, ces dernières permettant de se préserver et de conserver son indépendance sans être vulnérable.

« Points Clefs Formation »

Secteurs-clés de l'entreprise

Les risques de vulnérabilité pèsent essentiellement sur les secteurs clés de l'entreprise, à savoir :

- les infrastructures dites sensibles (Bureaux d'études, pôles de conception/assemblage) ;
- les télécommunications et autres moyens d'informations (internet) ;
- le personnel (permanent et temporaire) ;
- les relations publiques (visites de délégation) ;
- actions financières et boursières : OPA, rachat et liquidation de pans de la société.

L'entreprise *Ventili* prend en compte la réalité des risques auxquels elle peut être confrontée, en fonction de son secteur d'activité. Les principales menaces relèvent du domaine de l'électronique, avec les risques d'interception de données informatisées ou transmises oralement, le contrôle des informations sur Internet et le vol d'informations, de techniques et méthodes de production.

L'entreprise, dans sa démarche défensive, doit adopter trois concepts d'action : protéger son potentiel (ses compétences techniques, son savoir-faire, ses infrastructures), préserver son influence et, enfin, s'imprégner du schéma de pensée de ses principaux concurrents (perception management).

Mais Pierre Darmond souligne que le principe de précaution ne doit d'aucune manière nuire à la considération à l'égard des concurrents ; entre respect et méfiance : « En tout cas, il ne faut jamais les sous-estimer. Il est préférable de les considérer à leur juste valeur et de se méfier de leur propre stratégie de développement et des méthodes qu'ils sont prêts à utiliser pour atteindre leurs objectifs. »

En même temps, les différents chefs de service de *Ventili* étaient loin d'imaginer que la première menace qui devait les toucher de plein fouet provenait d'un service extérieur aussi courant…

Face aux services externes, aux interventions extérieures

Cela arriva en période de transition, en une fin d'année difficile et un faible redémarrage en janvier. Inquiet, Pierre Darmond avait alors le sentiment d'être confronté à un déficit chronique. Il craignait que *Ventili* ne tienne pas le choc et soit obligée de subir un plan social préventif, avec mise au chômage technique d'employés. Aussi, fut-il tenté d'accepter un nouvel actionnaire, étranger.

L'actionnariat étranger

Contrairement à ses habitudes, Darmond fit confiance, dans un premier temps, à un actionnaire européen. Mais, devant la facilité avec laquelle la collaboration semblait se sceller, Pierre Darmond eut un doute sur les motivations et surtout les finalités de la démarche de son correspondant. Il mit alors Eric Chatran sur l'affaire en lui demandant d'obtenir toutes les informations possibles sur cet actionnaire un peu trop conciliant. Quelques jours plus tard, Eric Chatran déposait sur le bureau de Pierre Darmond un dossier aux éléments fracassants : l'actionnaire européen était en fait une « couverture » d'un concurrent chinois qui s'appliquait à racheter des PME en mauvaise posture commerciale ou financière pour les restructurer, en devenant peu à peu actionnaire majoritaire, et en les remodelant dans son seul intérêt. Il s'efforçait d'en faire les relais de sa politique d'exportation sur le marché occidental. En l'occurrence, il s'agissait d'une société chinoise – un important producteur et vendeur chinois basé à Hong Kong – désireux, à terme, de licencier les deux tiers des effectifs de l'entreprise *Ventili* et de conserver uniquement le département Recherche. Devant une telle menace, Darmond mit fin aux relations avec l'actionnaire, évitant ainsi un péril bien plus grave que les difficultés auxquelles *Ventili* était temporairement confrontée.

« Points Clefs Formation »

La fiabilité des actionnaires en question

Il faut être prudent face à la démarche de tout actionnaire étranger. Dans un premier temps, il peut investir quelques millions d'euros salvateurs dans l'entreprise, gage de confiance et d'assurance. L'avenir peut alors paraître comme à nouveau prometteur. Pourtant, il peut arriver que la démarche de l'actionnaire se radicalise, notamment lorsqu'il s'agit d'un actionnaire majoritaire, en procédant à des licenciements et des restructurations – destructrices – de l'entreprise.

Une fois la menace passée, Pierre Darmond, soulagé, constate dans les semaines suivantes, une reprise des ventes qui arrive ainsi à point nommé. Alors que les chefs de services sont réunis dans son bureau, il tire le bilan de l'affaire, et remémore un autre épisode difficile qui contribua à conforter sa démarche en matière d'intelligence économique. Eric Chatran étant le dernier venu dans l'entreprise, il lui conte l'affaire, sous le regard complice des autres chefs de service qui acquiescent. Tous se rappellent de cet autre bien mauvais souvenir.

Comptabilités et ressources humaines : les risques de la sous-traitance

Deux ans auparavant, pour des raisons de simplification de son fonctionnement, Pierre Vermond en accord avec ses principaux collaborateurs, externalisa la gestion des Ressources humaines (voir plus loin) et la comptabilité de *Ventili*. Il fit appel pour cette dernière à une grande agence parisienne d'experts comptables. Or, l'agence gérait également les fonds d'un concurrent assez puissant, dont le siège social était implanté en Russie. Influencé par l'importance de son client, et effrayé devant les pressions psychologiques – et menaces – qu'il subissait, le comptable accepta de communiquer des informations sur la gestion de *Ventili*. Le concurrent, au terme de quelques mois, envisagea alors de racheter la petite société. A la fois surpris et suspicieux devant la connaissance que le concurrent avait de sa situation financière, Pierre Darmond fit peu à peu le rapprochement avec l'externalisation de son service de comptabilité. Aussi, pour en avoir le cœur net, sollicita-t-il les services d'une agence spécialisée dans l'intelligence économique. Une enquête fut menée, en toute discrétion, chez le comptable pour savoir ce qui se tramait. P. Darmond avait des doutes sur la discrétion de ce dernier car des informations normalement confidentielles avaient été divulguées auprès de

divers sous-traitants ; sous-traitants qui œuvraient également pour le concurrent russe… Finalement confondu, le comptable se confia, peu coutumier d'une telle situation conflictuelle et convaincu que tout cela devenait ingérable.

Pierre Darmond mit alors fin au contrat avec l'agence de comptabilité et décida de créer, en interne à *Ventili*, son propre service de comptabilité. Voulant éviter toute aggravation de l'affaire, Pierre Darmond préféra en rester là vis-à-vis du concurrent peu scrupuleux. Mais, il ne manqua pas de faire état de « l'incident » auprès de quelques contacts du ministère de l'Economie, des Finances et de l'Emploi, et d'un ami employé à la Direction générale de la Concurrence, de la Consommation et de la Répression des Fraudes (DGCCRF). La brigade d'enquête sur les fraudes aux technologies (BEFTI) fut également informée.

Pierre Darmond pensait en avoir fini avec les difficultés de ce type. Pourtant, peu de temps après, son entreprise fut confrontée à un nouvel incident comparable, au niveau de la sous-traitance en ressources humaines.

Conseillé par un ami entrepreneur dans un autre secteur que le sien, Pierre Darmond avait cru bon de se tourner vers un service externe en matière de Gestion des ressources humaines ; à une période où *Ventili* ne disposait donc pas encore, en son sein, d'un service analogue. Comble de malchance, la société de service à laquelle il s'adressa était guidée par le seul attrait financier. Elle se révéla dépourvue de toute éthique et respect élémentaire du secret professionnel ou de la confidentialité. Sous la coupe d'un important concurrent de *Ventili*, l'entreprise de gestion des ressources humaines n'hésita pas, contre de fortes indemnités, à communiquer les coordonnées d'employés de *Ventili* susceptibles de correspondre au profil d'actifs nécessaires au groupe concurrent. Une fois ce dernier renseigné, il ne lui resta plus qu'à entrer en contact avec les intéressés. Il leur fit des propositions séduisantes, sur le plan financier, pour les embaucher (ou débaucher…). En quelques semaines, *Ventili* perdit ainsi deux cadres et un technicien, motivés par les hausses de salaires et les avantages matériels que leur proposait ledit concurrent. Surpris d'une telle succession de départs en un laps de temps aussi réduit, Pierre Darmond, après avoir discuté de la situation avec ses collaborateurs, mena sa propre enquête. Il sollicita quelques proches œuvrant eux-mêmes dans l'intelligence économique. Ceux-ci contactèrent alors à plusieurs reprises les anciens employés de *Ventili*. Pierre Darmond recoupa les informations obtenues en parallèle. Il fit ainsi a lumière sur cette affaire…qui fut réglée devant les tribunaux… Car les employés débauchés avaient aussi apporté un certain savoir-faire directement tiré des activités de *Ventili* et qui servaient alors de faire-valoir. Finalement confondue, l'entreprise de gestion des

ressources humaines fut discréditée pour sa violation de la clause de confidentialité. Elle dut mettre la clé sous la porte, écrasée par une lourde amende et la perte d'intégrité de ses services. Quant au groupe concurrent, il dut également s'acquitter d'une forte amende. Mais il avait prévu un tel volte-face de *Ventili*. Si bien qu'il ne fut guère inquiété par les conséquences de cette affaire qu'il minimisa soigneusement.

« Points Clefs Formation »

Les employés de l'entreprise

Pour autant, il ne faut pas systématiquement se méfier des intentions des anciens employés mais tout simplement répondre à une méthode de préservation du pôle stratégique de l'entreprise. Ce pôle dépasse les individus en tant que tels. Mais il ne doit pas pour autant occulter le respect à la personne. On y revient toujours ! Par conséquent, il est donc louable d'appliquer une bonne gestion des moyens d'identification.

L'heureux aboutissement, pour *Ventili*, de ces affaires contribua à lui forger une image de société à la fois rigoureuse et vigilante. Elle démontra sa capacité à défendre efficacement ses intérêts propres. Du coup, les concurrents désireux de procéder à des démarches de déstabilisation furent quelque peu dissuadés. Ils redoutaient l'efficacité du pôle d'intelligence économique dont disposait à présent *Ventili*. Au sein même de l'entreprise, la manière avec laquelle furent gérés les problèmes posés par ces menaces contribua aussi à convaincre les derniers sceptiques quant à l'utilité du pôle d'IE.

De son côté, Pierre Darmond se félicita d'avoir recruté Eric Chatran et de pouvoir s'appuyer sur un solide réseau de relations extérieures.

Le principe des audits constitue par ailleurs de potentielles ouvertures susceptibles d'être exploitées par des concurrents. Deux cas de figure en témoignent.

Audit par un organisme externe

Devant la réussite de ses affaires, Pierre Darmond envisage d'obtenir la norme internationale ISO attribuée par l'Organisation internationale de normalisation (ou International organization for standardization en anglais), mise en place en 1947. Cette norme, appliquée dans les domaines industriels et commerciaux, peut en effet contribuer, estime Pierre Darmond, à la considération de *Ventili* sur le marché international.

Le secrétariat de direction de *Ventili* fait alors appel à un organisme spécialisé dans l'attribution de la norme ISO. *Ventili* fait donc l'objet d'un audit pour faire le point sur sa situation. Des représentants de l'organisme viennent à plusieurs reprises dans l'entreprise et prennent en compte tous les éléments nécessaires à la constitution du dossier. Au terme de l'étude, *Ventili* finit par obtenir l'ISO. Mais ni Pierre Darmond, ni aucun employé de l'entreprise ne sut qu'un membre de l'équipe chargée de l'audit, en avait profité pour établir un véritable bilan sur la situation économique de *Ventili* ; bilan qui fut communiqué à plusieurs de ses concurrents et qui leur permit de s'imprégner du niveau de puissance commerciale et financière de *Ventili*…

Autre situation appelant à la réalisation d'un audit : la signature d'un contrat d'assurance. Les services financiers de *Ventili* contactent un assureur qui accepte de couvrir l'entreprise de Pierre Darmond. Pour l'établissement du contrat, diverses informations sont transmises à l'assureur. En complément, celui-ci se déplace et obtient aussi des données chiffrées sur le personnel, les locaux, le mobilier, les biens de production. Autant d'éléments à intégrer dans le contrat. Eric Chatran fut chargé de suivre de près l'exploitation des informations recueillies par l'assureur. Cette fois, Pierre Darmond voulait éviter une nouvelle fuite de données. Pas question de laisser le champ libre à des indiscrétions motivées par la malveillance d'un concurrent. Le manque éventuel d'éthique et de professionnalisme de l'assureur pourrait bien conduire à la divulgation de renseignements confidentiels à quelque industriel curieux.

« Points Clefs Formation »

Sous-traitance et externalisation

Le recours au principe de la sous-traitance et de l'externalisation de certains services doit reposer, au préalable, sur une parfaite connaissance des interlocuteurs. Il faut privilégier des partenaires économiques dont les activités s'inscrivent dans un régime de transparence. Le professionnalisme des sous-traitants doit être intégral et sans faille. Dans le cas contraire, les conséquences peuvent être lourdes sinon désastreuses, à défaut de pouvoir se rendre compte assez tôt de la réalité du double jeu et des fuites qui peuvent s'effectuer à vos dépens.

Qu'il s'agisse d'un sous-traitant localisé en France ou à l'étranger, le principe de précaution doit être le même. Il est néanmoins plus délicat lorsque vous travaillez avec un sous-traitant étranger. Les impératifs de délais, de qualité des produits sont difficiles à estimer tant que les premiers résultats ne vous parviennent pas.

Il faut donc bien s'informer, se renseigner sur la réputation dudit sous-traitant. Et être à l'écoute… Connaissez-vous des industriels mécontents, insatisfaits ? Quelle est la santé financière de ce sous-traitant ? Qui dispose du capital ? Y a t-il un ou plusieurs actionnaires ?

Une fois que vous estimez disposer d'informations suffisamment larges et convaincantes, vous pouvez prendre votre décision quant au choix d'un éventuel sous-traitant. Tout doit reposer sur une confiance totale. Ne laissez pas la place au moindre doute, surtout si le sous-traitant travaille avec quelques-uns de vos principaux concurrents, français ou étrangers.

En bref…

Il faut avoir conscience d'être potentiellement vulnérable face à la concurrence.

Le contexte commercial est inscrit dans une dimension conflictuelle des relations économiques. Avec des actions de concurrence souvent impitoyables, voire déloyales. Celles-ci se traduisent par des missions de déstabilisation ou de neutralisation plus ou moins graves qu'il faut savoir anticiper en adoptant des méthodes de travail adaptées.

Les méthodes d'intelligence économique reposent avant tout sur un esprit de d'équipe et de cohésion, forgé par la communication et la transparence, en sachant placer les relations humaines au centre du dispositif.

La force de l'entreprise repose donc :

- sur la solidité d'un climat de confiance entre les différents acteurs ;
- sur la mise en valeur des compétences individuelles et collectives.

La capacité d'action des employés d'une entreprise, en parfaite concordance avec la direction, doit également témoigner de vigilance et de prudence dans les relations externes, avec le souci permanent de recouper l'information et d'éviter tout risque de fuite et de récupération de données capitales.

2) Protéger ses infrastructures et le personnel

On l'a vu avec les exemples précédents, le domaine du secteur tertiaire, avec la profusion à la fois des services et des clients, est une véritable plate-forme de menaces et de risques de fuite. Mais s'ajoutent à cette première série de menaces, les risques de violation des infrastructures, de vol de documents, sous quelque forme que ce soit. On peut aussi être exposé à l'infiltration de véritables espions au sein de l'entreprise. Autant de défis auxquels Pierre Darmond et son équipe sont confrontés.

A) Sécuriser les locaux

Face à l'espionnage et aux intrusions

En matière d'intelligence économique, les PME/PMI sont évidemment les maillons faibles. Eric Chatran, responsable de l'intelligence économique et des questions de sécurité de Ventili, le sait pertinemment. Elles sont d'autant plus vulnérables qu'elles misent généralement sur la recherche, l'efficacité sans pour autant se soucier de la protection des savoir-faire, du personnel et des infrastructures.

Initialement, la direction de Ventili ne prêtait pas d'attention particulière à la protection de son site. Jusqu'à ce qu'une effraction fut constatée au niveau de l'entrepôt de stockage des produits. Au cours de la même semaine, des vols furent enregistrés. Les enquêteurs de la gendarmerie, sensibilisés et formés aux problématiques sécuritaires des entreprises, ont relevé suffisamment d'éléments pour mettre en évidence quelques carences importantes dans la protection physique de l'entreprise. Ces militaires ont su convaincre le directeur qu'une autre approche de la sécurité devait prévaloir. Les constata-

tions ont de surcroit permis de remonter en quelques semaines aux auteurs des cambriolages.

Face à une telle situation, Pierre Darmond tint une réunion extraordinaire avec les chefs de service. Tous étaient convaincus qu'il fallait réagir rapidement et ne plus restreindre dès lors la politique de sécurisation. Des systèmes d'alarme furent installés pour prévenir toute nouvelle intrusion. Au niveau du magasin, un système de cartes d'accès fut instauré, limitant ainsi l'entrée aux seuls responsables des stocks et de leur gestion. Dans les bureaux d'étude et de l'administration de l'entreprise, des caméras furent placées au niveau des accès. Enfin, le port d'un badge fut instauré, d'un commun accord, entre la direction et les représentants du personnel.

Pierre Darmond et Eric Chatran voulaient ainsi trouver un compromis pour ne pas indisposer le personnel de ces services qui aurait pu croire à une mise sous contrôle de leur travail, avec toutes les dérives que cela peut toujours engendrer : vérifier le comportement au quotidien, quantifier les allers et venues. Il s'agissait en fait de ne pas basculer dans la psychose ni dans un climat de sécurisation excessive.

Une fois tout ce dispositif activé, les vols ne se renouvelèrent jamais plus. Pour la direction, il fallait éviter, par ce biais, toute intrusion dans les bureaux d'étude où un nouveau modèle de ventilateur était sur le point d'être lancé. Des plans, des données chiffrées auraient alors pu être dérobés. Avec toutes les conséquences que cela peut poser en matière de violation de la propriété intellectuelle, de probable copie du projet par un groupe concurrent ; en Asie par exemple…

« Points Clefs Formation »

Sécurisation interne et externe

Grâce à des lectures appropriées, à des informations reçues directement du ministère de l'Economie, les employés des PME/PMI – quelque soit leur poste de responsabilité – peuvent prendre conscience de l'importance de la notion de sécurisation et de protection. Cela vise à la fois les infrastructures, contre toute intrusion ou acte de malveillance, et le personnel lui-même, contre les pressions extérieures (chantage, corruption, détournement d'informations, etc.).

Une fois sensibilisée à la question, la direction d'une PME/PMI, si elle n'a pas les moyens financiers de mettre en place un système de sécurité interne, peut solliciter une société de renseignement privée (SRP) qui se charge de la sécurité économique de l'entreprise. Par principe, les SRP affirment ne jamais pratiquer

d'espionnage[3]. En revanche, leur action se focalise sur les informations sensibles, dite « grises », par rapport aux informations dites « noires » c'est-à-dire secrètes et d'importance stratégique pour l'entreprise.

Enfin, retenons que les principales catégories de risques sont les suivantes : vol d'informations, usurpation d'identité, intrusions et utilisations de ressources systèmes ; pillage des ressources informatiques ; mises hors service des systèmes.

Toute entreprise peut disposer de son propre système d'accès à l'information, en tenant compte des niveaux de responsabilités des collaborateurs. Par exemple au niveau informatique, la gestion administrative des entrées et sorties peut reposer sur l'usage de clés, de codes et de conventions. Ainsi, lorsqu'un employé change de fonction ou de responsabilité ou quitte même l'entreprise, il est préférable de modifier, par exemple, les codes et mots de passe pour éviter, à plus ou moins long terme, de graves désagréments. L'ancien employé pourrait communiquer ces codes d'accès ou en abuser par rancune.

Surveillance des locaux et du personnel

Compte tenu des risques qu'encoure une PME/PMI, il vous faut régulièrement procéder à l'inventaire des biens et tester le système de sécurité pour en relever les éventuelles failles.

Instauration de règles de sécurité

Pour mesurer la qualité des systèmes de sécurité de *Ventili*, Pierre Darmond et Eric Chatran décidèrent en fin de journée de simuler eux-même des intrusions, tandis que deux collaborateurs, depuis le poste de sécurité et de surveillance des locaux, enregistraient la réactivité des systèmes informatiques et vidéos. Tous les tests furent probants et l'alarme fut à chaque fois donnée en cas d'intrusion dans des secteurs théoriquement clos. Au niveau du magasin, P. Darmon décida de prendre quelques pièces, afin de voir si les magasiniers tenaient bien la gestion de leur stock.

Deux jours après les faits, le chef magasinier informa la direction que des pièces avaient disparu. Pierre Darmond se félicita de cette rigueur professionnelle, du bon suivi des stocks et de l'efficacité générale du système de surveillance de son entreprise.

3) En France, nombre d'anciens agents de la Direction de la sûreté territoriale (DST) ou de la Direction générale de la Sécurité de l'Etat (DGSE) intègrent ce type de sociétés. Certains sont même à leur origine.

Pour être certain que tout est bien « verrouillé », Pierre Darmond, depuis son domicile et grâce à l'ordinateur de son fils, entra en contact avec le service informatique de *Ventili*. Il se fit passer pour un journaliste économique désireux d'obtenir des informations sur les activités de l'entreprise. Pierre Darmond venait de faire embaucher, depuis peu, un jeune informaticien ; l'occasion par conséquent de sonder sa conscience et sa discrétion professionnelles. Pierre Darmond, une fois le contact établi, obtint tout d'abord, conformément à sa demande, des informations générales sur *Ventili*. Puis, au fur et à mesure, il demanda des données de plus en plus sensibles, notamment sur les perspectives de développement de *Ventili*, l'ambiance au sein de l'entreprise, etc. Avec naïveté, le jeune informaticien révéla ce dont il avait entendu parler et confia sa perception de la vie de l'entreprise. Certes, cela permit à Pierre Darmond de voir que l'ambiance globale était satisfaisante. Mais l'indiscrétion du jeune informaticien était évidemment inquiétante dans l'absolu. Après plusieurs jours de ce type d'échanges, Pierre Darmond convoqua l'informaticien et lui révéla toute la dimension de leur contact par mails. Le jeune homme fut estomaqué. Il n'avait pas pris conscience de la vulnérabilité de l'entreprise en diffusant ainsi des informations qui, au premier abord, lui semblaient anodines. Compréhensif, Pierre Darmond mit en garde le jeune actif pour qu'à l'avenir il se montre nettement plus réservé et prudent. Jamais plus un tel incident ne se reproduisit. En effet, Eric Chatran, quelques mois plus tard, mit à l'épreuve l'intéressé par mails. Cette fois, l'informaticien évita de divulguer des informations sensibles ou délicates. La leçon avait porté ses fruits…

« Points Clefs Formation »

Savoir tester ses moyens de sécurité

Une fois que vous avez établi des moyens de sécurité et de surveillance, après quelques temps d'application de votre système, sondez vous-même son efficacité et les réactions de certains de vos collaborateurs qui, par exemple, travaillent avec l'extérieur principalement par informatique. Vous pouvez mener des actions préalables dites d' « ingénierie sociale » qui consistent à vous faire passer pour une tierce personne en quête d'informations confidentielles. Vous pourrez jauger le degré de prudence, de méfiance et de perspicacité des employés « testés ».

Dans le même ordre d'idées, les moyens de sécurisation des échanges, des données sensibles (fichiers clients, brevets, plans, etc) doivent, eux aussi, être

revus en permanence. Il faut d'ailleurs être encore plus vigilant lorsqu'il y a risque d'accès au réseau en interne comme externe, par des personnes non autorisées. Les échanges sur Internet doivent alors faire l'objet de protocoles sécurisés, de même que les échanges de données confidentielles. Quant aux certificats, il faut s'assurer de la confidentialité des notions de bases, de l'instauration d'une signature électronique infalsifiable et de l'instauration d'un chiffrement.

On imagine la situation si des éléments confidentiels sont interceptés par un élément extérieur qui peut les réutiliser à son profit, les revendre à un de vos concurrents… Il n'y a alors plus rien à faire. Si ce n'est tenter de mesurer les conséquences en vous appliquant à capter les évolutions de vos concurrents.

Préserver la communication et l'accès à l'information

Pierre Darmond ne cesse de le répéter : sa volonté de renforcer le pôle de renseignement de *Ventili* ne doit pas se traduire par une informatisation à outrance de ce service. Le facteur humain doit demeurer au cœur de l'organisation. Mieux vaut réduire, estime-t-il, avec l'approbation des diverses

« Points Clefs Formation »

La politique de sécurité de l'entreprise : pourquoi faire ?

La politique de sécurité propre à votre entreprise repose, tout d'abord, sur l'estimation des biens à protéger et les risques qui y sont liés. En même temps, tout le personnel doit être sensibilisé au nécessaire respect des règles de sécurité.

Cela est impératif car l'entreprise est tenue à des obligations légales, conformément aux lois, règlements et accords professionnels qui peuvent engager la responsabilité du chef d'entreprise. C'est particulièrement net lorsque des dommages sont causés aux tiers. La responsabilité de l'employeur est alors engagée lorsque, par exemple, l'un de ses salariés consulte un site internet illicite, viole sciemment le droit d'auteur ou procède à des opérations frauduleuses par le biais de l'outil informatique notamment. Enfin, de graves dommages peuvent être causés à l'entreprise, notamment en cas d'atteinte à la confidentialité ou la modification des données comptables.

Toutes ces situations doivent interpeller les responsables d'une entreprise et les inciter à connaître le régime général de responsabilité qui est applicable, de même que les règles des contenus informationnels et d'utilisation des moyens de communication électronique.

directions de service, les risques de fuite, de perte ou d'interception de données dites confidentielles en sensibilisant le personnel. Avec la conviction permanente que l'information est précieuse. Elle est en effet un bien qui doit être préservé et non diffusé auprès de personne non accréditée.

Il existe une catégorie de personnels qu'il faut a priori suivre avec précaution : les responsables d'entretien et de maintenance du matériel bureautique.

Le personnel de maintenance et d'entretien

Chez *Ventili*, comme dans n'importe quelle autre entreprise, il est impossible de se passer des services de maintenance ou d'entretien ; le réseau d'électricité, le « parc » de photocopieuses, sans oublier les sanitaires et toilettes ni l'entretien des bureaux et des ateliers.

Comme à l'accoutumée, *Ventili* fait donc appel à de petites sociétés de service qui, régulièrement, viennent entretenir ou contrôler le matériel. Alors que l'une d'elles envoyait systématiquement les mêmes techniciens pour le nettoyage des locaux, plusieurs secrétaires s'étonnent de voir, un jour, un nouveau venu parmi eux.

Se souvenant des appels à la vigilance d'Eric Chatran lors de la dernière réunion interservices, les secrétaires veillent à ne laisser sur les bureaux aucun document sensible ou confidentiel. Et elles ferment soigneusement tiroirs et armoires. Pourtant, le lendemain, l'une des secrétaires se rend compte que des documents ont été déplacés, qu'une armoire de son bureau, pourtant fermée, a été ouverte. Justement après le passage du personnel de nettoyage.

Par un appel téléphonique au sein de la société de nettoyage, Eric Chatran apprend avec stupéfaction que le soit disant nouvel employé ne fait pas partie de leur antenne mais aurait été envoyé par une branche associée… Désireux de confirmer ses craintes, Eric Chatran laisse sur son bureau des documents – sans importance – et glisse même un cheveu au milieu des quelques feuilles. Le lendemain, en reprenant les documents empilés, il constate que leur ordre n'est plus le même et que le « cheveu témoin » a disparu. Preuve que les documents ont été consultés…Devant ce cas de vol caractérisé d'informations, la direction, une fois prévenue, procède à l'installation d'une mini caméra. Parfaitement dissimulée, elle enregistre ce qui se déroule le soir dans le bureau, à l'heure ou le personnel d'entretien travaille. Et là, le nouveau venu de l'équipe d'entretien est filmé en train de fouiller non seulement les dossiers mais aussi de tenter de consulter les fichiers informatiques de l'ordinateur du bureau (ce qui se révéla impossible car l'accès était verrouillé par un mot de passe). Confondu, le coupable doit répondre de ses actes devant la justice. Après enquête, il s'avéra que le « suspect » avait infiltré la société d'entretien en se faisant embauché quelques mois, le temps

nécessaire pour venir à plusieurs reprises au sein de *Ventili*. Il n'était évidemment pas un employé d'entretien courant, puisqu'il s'agissait d'un spécialiste de l'espionnage industriel. Au sein de *Ventili*, il devait même procéder à la fouille minutieuse des poubelles, à la copie de documents. Il livra le nom de son commanditaire : un groupe concurrent… Mais Pierre Darmond ne put intenter le moindre procès au groupe concurrent, par faute de preuves. Leur « agent » n'avait pas eu le temps suffisant pour mener son plan à exécution.

« Points Clefs Formation »

Le principe de précaution doit ainsi s'étendre aux techniciens de surface plane, autrement dit les « femmes de ménage » et autre personnel de nettoyage.

Dans une autre situation, Eric Chatran se rendit compte que les deux techniciens chargés de la maintenance des photocopieuses revenaient un peu trop souvent, sous prétexte que lesdites photocopieuses présentaient des problèmes récurrents. Intrigué, il découvrit qu'en fait, les employés de la petite entreprise de maintenance venaient récupérer les « mémoires » de mini capteurs photographiques qui avaient enregistré tous les documents photocopiés par le personnel administratif de *Ventili*. Une fois reproduits, les documents étaient vendus à un concurrent russe. Cette affaire fit, par contre, grand bruit.

« Points Clefs Formation »

La technologie au service de l'espionnage industriel

Il faut être vigilant quant à la nature même des personnes chargées de missions spécifiques dans l'entreprise.

Il existe une multitude de moyens technologiques qui rendent possibles, pour n'importe quelle personne informée de leur utilisation, toute activité « d'espionnage » : entre micros, écoutes téléphoniques, caméras miniatures, stéthoscopes, exploitation des informations conservées dans les puces RFID – d'à peine un millimètre d'épaisseur – (qui permet également le traçage à distance).

L'une des concrétisations de l'espionnage les plus en vues est vraisemblablement celle des écoutes téléphoniques.

Les écoutes téléphoniques

Annie Baral, responsable de la Communication et Alain Pautrat, responsable de la Gestion de production, n'avaient jamais de souci avec leur téléphone. Jusqu'au jour où, à plusieurs reprises, ils s'étonnèrent d'entendre des grésillements et une double tonalité en décrochant leur combiné. Parfois même un très léger sifflement se faisait entendre. Ils firent part de la situation à Eric Chatran qui procéda alors à quelques tests électroniques sur leur ligne avec un matériel adapté. C'est ainsi qu'il découvrit que les lignes des deux directeurs de service de *Ventili* étaient sur écoute. Avec Pierre Darmond, il fit alors procéder à un contrôle de toutes les lignes téléphoniques et des combinés pour repérer micro et émetteur clandestins. Enfin, les éléments détectés furent neutralisés mais jamais ils ne surent qui était à l'origine de cette situation flagrante d'espionnage. Ils purent seulement se rassurer en observant qu'il s'agissait d'amateurs. Leur maladresse et les « bruits témoins » avaient attiré l'attention.

Depuis, le contrôle des lignes téléphoniques est effectué régulièrement.

« Points Clefs Formation »

L'espionnage téléphonique, source de toutes les dérives

L'entreprise et ses cadres les plus importants peuvent être exposés à des procédures d'écoute téléphonique accomplies par des groupes étrangers. Les micros peuvent être dissimulés soit dans le bureau des personnes, soit dans le combiné du téléphone, ou encore caché dans le revers d'une veste, d'un manteau, la couture d'un cartable, etc. Seul le passage des locaux au détecteur et une fouille minutieuse – ce qui nécessite de faire appel à des spécialistes – permettent de découvrir une procédure d'écoute sauvage. On peut aussi essayer de faire des recoupements après avoir observé, semaines après semaines, la mise en échec, par exemple, de projets commerciaux ; en constatant que l'on est régulièrement devancé par des concurrents auprès de ses propres clients.

Retenons que le recours aux écoutes téléphoniques est strictement interdit dans le cadre privé. Pour sa part, la Justice procède à des écoutes téléphoniques à hauteur de 30 000 par an, en moyenne.

Malgré des règles juridiques très strictes en la matière, le recours aux écoutes téléphoniques, de façon illégale donc, est néanmoins répandue et source de toutes les dérives possibles. Pour un chef d'entreprise, c'est parfois la tentation – clairement inacceptable – de procéder à l'espionnage de certains de ses

cadres pour des raisons d'ordre privé ; loin, par conséquent, d'hypothétiques craintes au niveau professionnel. Ne parlons même pas de celles inscrites dans les dérives du harcèlement moral et sexuel. Le problème est pourtant de taille et bien réel actuellement en France.

La vidéo surveillance : précautions d'emploi

Depuis que le terrorisme est devenu une menace tangible, les systèmes de vidéosurveillance ont eu tendance à gagner les entreprises au même titre que les structures ministérielles et l'ensemble des services publics.

Motivé par la démarche de certains de ses collègues entrepreneurs, Pierre Darmond décide lui aussi de doter son entreprise d'un système de surveillance vidéo important. Ainsi, outre les entrées des bâtiments et les quelques lieux considérés comme stratégiques, il veut équiper à leur tour les divers espaces de travail d'un système de vidéo. Mais cette démarche est mal accueillie par une minorité du personnel inquiète à l'idée d'une dérive vers le tout sécuritaire. La direction met alors en avant l'opportunité d'élargir le champ vidéo au-delà des seuils d'accès à l'entreprise pour des raisons de sécurité des employés, notamment dans les ateliers d'assemblage des ventilateurs. En outre, elle souligne l'économie d'échelle qui résulte de la multiplication des caméras. Mais le comité d'entreprise estime finalement que les mesures de sécurité établies, conformément à la charte du travail et aux lois professionnelles, sont tout à fait suffisantes et ne nécessitent donc pas l'extension outre-mesure du réseau de vidéo surveillance. De surcroît, la Commission nationale de l'informatique et des libertés (Cnil), obligatoirement sollicitée pour donner son avis sur un tel projet, émet un avis négatif puisqu'il ne s'agit pas d'un domaine d'activités sensibles. Pierre Darmond se plie alors aux directives publiques et le projet d'extension fut abandonné.

« Points Clefs Formation »

Les limites de la surveillance vidéo

Systématiquement, il est primordial de protéger les libertés individuelles et de respecter la vise privée des salariés ; si bien que l'autorisation d'une vidéo surveillance dans les bureaux, ou au niveau de la machine à café sera toujours refusé.

Aussi, la direction peut-elle, si elle l'estime opportun dans le cadre de ses activités, procéder à la protection des données, en mettant en place l'utilisation de clés d'accès, de systèmes de cryptage, de connexions sécurisées ou encore de filtres internet.

A l'inverse, la direction peut choisir d'installer une vidéosurveillance dans des locaux où les salariés ne doivent pas se rendre, sauf sur autorisation spéciale.

En dehors de la protection des locaux et, de manière plus large, du site de l'entreprise, il faut aussi appliquer quelques mesures de précaution au niveau du personnel et, par extension, des clients, visiteurs et candidats à l'embauche.

B) Bien connaître son personnel

Gestion du personnel, des employés, des collègues

Pierre Darmond et Michèle Attenet, responsable des Ressources humaines, sont convaincus de l'importance de bien connaître les personnes avec lesquelles *Ventili* est appelée à travailler. Les renseignements humains sont, à ce titre, précieux et de plusieurs natures : entretiens réguliers ou impromptus, visites médicales, évaluations annuelles, suivis de carrière, attention portée aux comportements et aux éventuels changements d'attitude.

Michèle Attenet et les autres chefs de service sont d'accord pour dire que le « feeling psychologique », le sens des relations humaines est avant tout le meilleur atout pour désamorcer une crise, un malaise ou des malentendus.

« Points Clefs Formation »

Connaître parfaitement les membres du personnel

Bien cerner son personnel, ses collègues, c'est aussi témoigner d'une parfaite immersion dans son cadre professionnel.

Certes, cela peut se révéler insuffisant surtout si des doutes persistent. Il est possible alors de procéder à une surveillance assidue, si l'on pressent la fuite de secrets industriels, de détournements de marchandises. Mais, ce recours doit être extrême et exceptionnel : la déontologie réprouve toute dérive liée à une antipathie relationnelle, toute obstination à désarçonner un collaborateur pour des raisons personnelles et donc liées à la subjectivité et l'affectivité. Prendre les gens « comme ils sont » doit faire partie des principes-clés dans la vie sociale. Un principe qui, aujourd'hui, est pourtant de plus en plus déprécié et oublié.

Prudence dans les phases de recrutement

Embauche d'un nouveau collaborateur

Les phases de recrutement, pour *Ventili*, comme pour toute entreprise, sont des périodes déterminantes autant que sensibles. Michèle Attenet, responsable des Ressources humaines, prend donc très au sérieux ces moments de « sélection ». A terme, ceux-ci contribuent à fortifier l'équipe avec l'intégration d'un nouvel actif reconnu pour son potentiel professionnel. Par définition, il s'agit d'un apport substantiel au dynamisme de l'entreprise. Il est donc logique d'être à la fois exigeant sur la personne recrutée mais aussi attentif quant à sa fiabilité, surtout dans des secteurs particulièrement marqués par la concurrence.

Et lorsque l'on demande à Michèle Attenet sa méthode de recrutement, elle répond qu'elle ne choisit pas un postulant en fonction de ses seuls diplômes. Elle est également attentive à son expérience antérieure dans la conception/production de ventilateurs. Eric Chatran lui précise alors de vérifier consciencieusement les informations communiquées par le candidat. Car ce dernier peut très bien se targuer d'avoir une expérience professionnelle qui, en réalité, n'existe pas. Pourtant, en dépit de leurs précautions, Eric Chatran comme Michèle Attenet eurent à faire face à un autre cas de figure difficilement décelable.

En effet, un candidat, retenu parmi les trente potentiellement capables, brillait par son imposant savoir-faire et sa parfaite connaissance du marché de la ventilation. Après quelques entretiens, il apparaissait clairement que ce

candidat si doué faisait l'unanimité. Restait à organiser un ultime entretien avec Pierre Darmond, pour valider ou non son embauche au sein de *Ventili*. Mais Eric Chatran, pour être certain de la fiabilité du candidat, cherchait conjointement à savoir si le candidat était lié ou non à un groupe concurrent. Après quelques semaines d'enquête, il découvrit ainsi qu'officiellement ledit candidat avait été licencié par un des concurrents de *Ventili* mais qu'en réalité, il demeurait en contact étroit avec sa direction. En fait, il avait été détaché de son entreprise afin de pouvoir incorporer *Ventili*, d'en assimiler les principes de fonctionnement et d'y capter toutes les informations jugées nécessaires pour servir les intérêts du concurrent. A terme, cela pouvait conduire à un véritable affaiblissement de *Ventili*. Eric Chatran s'empressa de faire part de la situation à Pierre Darmond qui, en accord avec Michèle Attenet, écarta

« Points Clefs Formation »

Le recrutement, une opération délicate

Lors de l'embauche d'un nouveau collaborateur, la prudence doit être de mise. Il faut connaître précisément son expérience et son passé professionnels, sa situation au moment de l'entrée de votre l'entreprise, ses objectifs et perspectives. Car, il arrive qu'un concurrent licencie officiellement un employé pour que celui-ci postule ensuite auprès de votre entreprise, avec l'objectif de pouvoir ainsi y capter des informations confidentielles. Derrière un statut sans surprise peut donc se cacher un individu qui, finalement, s'imprègne de votre organisation globale, pour mieux cerner la politique de production de l'entreprise, du programme d'ouverture à l'international, etc.

Tout est possible en matière de personne douteuse ou malhonnête.

Il vous appartient donc de recouper vos sources d'informations, quitte même à rencontrer les anciens employeurs pour valider votre avis. Insistons d'ores et déjà sur la nécessité – récurrente – de « recouper » l'information : la confirmer par des éléments de foi, ou l'infirmer par des preuves incontestables. En aucun cas – d'où la difficulté de l'exercice – ne doivent interférés des jugements partisans. Or, il n'est pas rare de recevoir de mauvaises informations, sur un candidat, de la part d'un ancien employeur dépourvu d'honnêteté intellectuelle et dont l'éthique relationnelle est détestable.

Evidemment, si vous constatez que le candidat a travaillé auparavant chez un de vos concurrents directs, il faut être vigilant ; surtout si ledit concurrent connaît une situation conjoncturelle relativement défavorable. Il pourrait alors, dans un contexte de tensions commerciales, tenter de connaître insidieusement vos perspectives de développement.

définitivement le dangereux candidat.

Autre catégorie potentiellement à risque : celle des stagiaires.

La place des stagiaires

Le Service des Ressources humaines de *Ventili* reçoit en moyenne des dizaines de CV sinon par jour, au moins par semaine. Or, selon les statistiques officiellement établies en France, la moitié des CV présentent des anomalies, des falsifications. Il est vrai que sur Internet, il est même possible d'acheter de faux diplômes. Ils comportent des mentions, estampilles et fausses signatures de responsables et directeurs des Ecoles ou Structures de formation. Difficile, dans ce cas, d'y voir clair…

De même, il n'est pas aisé de déceler au préalable un candidat qui est un habitué du vol dans les caisses ou qui pratique assidûment la politique de négociation de départ tous les deux ans. Sauf si, une fois encore, la Direction met en avant l'importance du renseignement humain en s'informant en amont sur les antécédents dudit candidat. Elle peut alors confronter les données du candidat avec les informations obtenues indirectement (auprès des cabinets de recrutement, d'anciens collègues de l'intéressé, etc.).

Eric Chatran, une fois de plus, était là pour veiller au pire. Et la pertinence de ses méthodes d'investigations lui a permis de découvrir la vraie nature d'une stagiaire chinoise entrée depuis peu chez *Ventili*. Comme elle s'était bien adaptée et faisait preuve de dynamisme et d'initiative, des tâches assez importantes lui furent rapidement confiées. Or, Eric Chatran la surprit en train de consulter des dossiers qu'elle n'avait en aucune manière l'autorisation de prendre en compte. Son ordinateur portable fut fouillé et l'on découvrit de multiples copies de dossiers confidentiels sur la production et les ventes assurées par *Ventili*. Autant de documents qui étaient destiné à l'envoi électronique vers un destinataire chinois… Une fois de plus, l'affaire fut jugée devant les tribunaux. Elle contribua à alimenter le sentiment de potentielle vulnérabilité de l'entreprise face à des éléments « hostiles » intégrés – temporairement ou non – dans sa propre structure.

« Points Clefs Formation »

Encadrer et surveiller les stagiaires

Par définition, le stagiaire doit être rigoureusement encadré et cantonné à des tâches précises sans être « un touche à tout », une petite main pratique pour un entrepreneur peu scrupuleux et qui souhaite ainsi disposer d'un jeune actif potentiel pour combler temporairement son manque de personnel.

■■■ Il y a donc nécessité de respecter le stagiaire à sa juste valeur, sans l'exploiter, et lui permettre de s'épanouir dans un domaine précis. Mais, insistons sur ce point, il doit pour cela être clairement suivi – coaché pour reprendre un terme répandu – par un cadre de l'entreprise.

Le plus délicat est la période qui s'ouvre après plusieurs mois de présence dans l'entreprise. Les mesures de précaution s'estompent, le stagiaire n'étant plus considéré commun un élément exogène de l'entreprise. Et c'est là qu'en cas de malveillance préméditée de la part du stagiaire, il peut y avoir vol d'informations, notamment dans le domaine de transfert de technologie.

A travers ces diverses catégories de personnes potentiellement menaçantes pour l'entreprise, on perçoit nettement l'importance de tout organiser selon des principes de précaution. Chaque employé de l'entreprise, à son niveau, doit veiller à ne pas laisser « traîner » des documents sensibles (notes financières, rapports, conclusions d'entretien de partenariat, etc.). Une rigueur méthodique autant que naturelle – du moins doit-elle tendre à la devenir – qui concerne aussi les lieux publics : la discrétion doit rester de mise, notamment en matière de conversation téléphonique dans les trains. La consultation de documents est tout aussi délicate car les papiers sont susceptibles d'être égarés ou volés. C'est pourtant ce qui arriva à un cadre subalterne du service commercial de *Ventili*.

La phase délicate des voyages

Sans aucune précaution d'usage ni aucune discrétion, le cadre de *Ventili*, Frédéric Auchoir, revient d'un voyage à Paris, par le train. Il s'empare de son téléphone portable et, installé tranquillement dans son siège, appelle son épouse. Satisfait des négociations rondement menées, il s'en félicite et dévoile toute leur portée. Ces négociations concernaient un important client qu'il a vu le matin même. Sans réfléchir, il précise le volume de pièces prévues dans la commande et la valeur du montant qu'il a pu obtenir au terme de négociations serrées.

Il ne se doute même pas que parmi les autres voyageurs du wagon, se trouve un commercial d'un groupe concurrent qui prête l'oreille. En quelques minutes, il dispose de toutes les informations essentielles. Il prétexte un déplacement pour aller aux toilettes, jette au passage un regard attentif sur les documents que le cadre de *Ventili* a déployé devant lui, sur sa tablette. Le logo de l'entreprise apparaît clairement, permettant ainsi au curieux concurrent de voir à qui il a à faire. Quelques instants plus tard, il téléphone à sa direction, depuis une plate-forme entre deux wagons. Il met alors au point une opération commerciale à l'égard du même client de *Ventili*. Le but étant

de lui proposer, pour le même prix, des ventilateurs qui apparaîtront plus performants.

En fin d'après-midi, c'est chose faite. Le commercial fait parvenir un fax au client et double cette première approche d'un appel téléphonique au directeur. Sensible à la dimension « rapport qualité/prix », ce dernier finit pas annuler la précommande passée avec *Ventili* pour signer avec le concurrent. Ce dernier profitait ainsi d'une grave faute professionnelle de l'agent commercial imprudent.

Si, on l'a vu, on peut craindre les indiscrétions qui profitent aux groupes concurrents, ceux-ci peuvent aussi tenter d'intimider ou de corrompre quelques-uns de vos propres collaborateurs.

Les tentatives de corruption ou d'intimidation

La direction de *Ventili* s'assure en permanence que les cadres et ingénieurs, véritables piliers de la société, ne soient pas victimes de démarches d'approche de concurrents. Il y eut des antécédents qui ont contribué à rendre toute l'équipe prudente. Tous se souviennent en effet des tentatives de débauchage de deux cadres. Ceux-ci s'étaient vus proposer de salaires largement supérieurs. Mais ce sont surtout les pressions psychologiques subies par l'ancien directeur du Secteur de la Recherche qui sont restées dans les mémoires. Déstabilisé, en raison des menaces qui pesaient sur ses proches, il avait du transmettre des données confidentielles à un concurrent. Puis, il s'en était confié à Pierre Darmond. De connivence, il avait alors communiqué au dangereux concurrent de fausses informations et forcé ses intermédiaires à s'exposer jusqu'à qu'ils soient arrêtés.

Un cas similaire s'était produit pour un technicien. Marié, il fut approché par une femme qui, en réalité, était destinée à le séduire et à procéder, par la suite, à un chantage affectif, en le menaçant de tout dévoiler à son épouse. Après une période où le technicien accepta de subir cette pression, il finit par la révéler à sa direction qui fit bloc autour de lui. Une action assez complexe fut alors menée pour confondre la « mystérieuse séductrice » qui, au final, se révéla, une fois de plus, une professionnelle au service d'un groupe concurrent. Restait au technicien, écrasé de culpabilité et de honte, à régler le malaise avec son épouse…

Lorsque les médias s'en mêlent

Sur un autre plan, *Ventili* fut aussi la cible d'une campagne de désinformation, véhiculée par des médias qui s'appliquaient, de connivence avec un groupe concurrent de *Ventili*, à ternir son image de marque. Les informations

« Points Clefs Formation »

Exposé au double-jeu

Une fois encore, le facteur humain est essentiel ici. Vous pouvez en effet rencontrer un individu ou une femme qui, en fait, procède à une première approche pour vous « accrocher ». A terme, la personne peut obtenir des informations sans que vous en soyez nécessairement vous-même au courant. A votre insu, elle peut procéder à une récupération ciblée d'informations en votre possession, par le biais notamment de votre PDA ou de votre ordinateur portable. Elle peut aussi s'appliquer à suivre vos déplacements sur quelques semaines, tenter de connaître votre clientèle, etc.

Un problème d'ampleur nationale

Dans les PME-PMI liées aux activités sensibles, il est de plus en plus fréquent que le personnel disposant d'informations capitales soit l'objet de pressions extérieures. Au point que, depuis 2005, la Direction Centrale des Renseignements Généraux (DCRG) a mis en place une antenne spécialisée pour suivre 934 entreprises et s'assurer que les cadres n'avaient pas été soumis à d'éventuelles débauches. De même, les vérifications portaient sur les piratages ou vols d'ordinateurs. Les conclusions publiées au terme de 7 mois d'enquête ont révélé que 158 PME/PMI étaient considérées comme partiellement vulnérables et que 87 d'entre elles avaient subi directement des « actions hostiles » .

Les secteurs les plus touchés concernent la métallurgie, l'agroalimentaire, la chimie-plasturgie, l'informatique et le nucléaire.

De son côté, la Gendarmerie nationale, qui contribue au renforcement de la sécurité des entreprises, a mis en évidence les vulnérabilités du secteur de l'automobile et de l'aéronautique, soumis a des attaques répétées : accès frauduleux au système informatique, vols de matériels spécifiques, intrusion dans les locaux de production…

Sans faire une fixation disproportionnée sur l'économie chinoise, il est clair que Pékin diligente une offensive généralisée en vue d'une extension des intérêts chinois et des prises de contrôle élargi de pans entiers des économies d'Occident. De surcroît, la Chine est considérée comme l'espace-clé en matière de contrefaçons, notamment de produits de luxe.

4) J.-M. P. « L'espionnage économique menace les PME » in Le figaro, 30 novembre 2005

véhiculées se faisaient les relais d'une rumeur sur la mauvaise qualité de ses produits. Elles soulignaient des problèmes récurrents de gestion, une exploitation du personnel par une direction soupçonnée de malversations. Tout était faux. Mais les conséquences furent à la fois inquiétantes et immédiates : tensions au sein de l'entreprise ; doutes du personnel à l'égard de la direction ; mauvaise image de marque de Pierre Darmond ; perte d'influence de et de *Ventili* sur le marché.

Pierre Darmond engagea une importante contre-attaque en communication pour rétablir à son avantage la situation. Dans un premier temps, il rassura certains employés et prouva qu'il n'y avait aucune malversation et autres jeux financiers obscurs. Ensuite, il entama une véritable campagne à l'encontre de cette vaste diffamation dont *Ventili* était l'objet. Elle put être finalement annihilée mais au terme d'une longue procédure judiciaire.

Vis-à-vis du grand public, il fallut plus de temps pour relancer la demande. Ce qui porta malgré tout un lourd préjudice sur les ventes et l'image de marque de *Ventili*. Cela peut nécessiter plusieurs mois voire plusieurs années avant que *Ventili* ne retrouve une place satisfaisante sur le marché de la ventilation. *Ventili* tentera de réhabiliter son image de marque notamment par une coûteuse campagne de communication et de presse.

Elle put en parallèle, en vertu de l'enquête d'Eric Chatran, remonter à la source de cette campagne de discrédit : un consortium de concurrents russe et chinois qui désirait accaparer le marché de *Ventili* en affaiblissant la PME française.

« Points Clefs Formation »

Face aux rumeurs et diffamations

Le discrédit peut viser soit l'entreprise, soit son directeur via une campagne de diffamation et de déstabilisation. Il faut alors au chef d'entreprise un solide sang froid pour pouvoir prendre du recul par rapport à la désinformation. Cette dernière peut néanmoins perturber les proches et les employés eux-mêmes, en créant le doute dans les esprits. Est-ce vraiment un homme qui a détourné des fonds, est-il coupable de trafics d'influence, mène-t-il vraiment une double vie ? etc.

Quoiqu'il en soit, l'apaisement et le retour à la normale nécessitent un long travail de fond, en faveur d'une véritable réhabilitation.

Ce qui nous conduit à aborder, à présent, un autre thème majeur pour la vie économique de l'entreprise : celui de l'information et de la communication au cœur, par définition, des activités socio-économiques.

3) Maîtriser et sécuriser le pôle informatique

Au gré des points abordés précédemment, on l'a constaté à maintes reprises, l'élément informatique est devenu un outil incontournable. Tant dans la vie privée que le domaine professionnel. Et l'évolution permanente des vecteurs informatiques conduit aussi de plus en plus d'actifs à « rapporter du travail » à domicile grâce aux ordinateurs portables. Mais cela ne doit pas rendre pour autant les employés « corvéables à merci » pour l'entreprise.

A) Un outil potentiellement vulnérable

L'employé qui dispose ainsi d'informations, s'expose, notamment dans les lieux publics, à d'éventuelles tentatives de saisies de ses données. Cela peut se révéler catastrophique lorsqu'il s'agit d'informations précieuses pour la stratégie de l'entreprise.

C'est pourquoi Pierre Darmond et Eric Chatran ne manquent pas d'appeler à la vigilance et l'extrême prudence des détenteurs d'ordinateurs portables. De même, sensibilisent-ils les utilisateurs de postes informatiques sur les risques liés au recours à l'Internet. Malgré tout, la direction de *Ventili* déplora plusieurs incidents.

Les manipulations à risques

Les échanges par Internet

Jacques Letourneur, informaticien et passionné par son travail, est technicien au Département Recherches de *Ventili*. Motivé par les multiples possibilités proposées par l'Internet, il décide de tenir un journal professionnel qu'il met en ligne en créant son blog[5]. Son site personnel dévoile

ainsi une véritable chronique sur le milieu de l'entreprise *Ventili*. Grâce à un système de lecture perfectionné, il met à jour tous les commentaires des personnes qui visitent son site. Et parmi eux, un informaticien d'un groupe concurrent, fin psychologue, procède à une opération d'approche de J. Letourneur. En usant de flatterie et d'une passion affichée pour les ventilateurs de *Ventili*, il réussit peu à peu à créer un lien régulier avec Letourneur au point de lui sous-tirer insidieusement des informations techniques. Sans que cela n'éveille le moindre soupçon de l'employé de *Ventili*. De telle sorte qu'il divulgua des informations qui devaient logiquement restées confidentielles.

« Points Clefs Formation »

En bref…

- En permanence, la direction a le souci de protéger à la fois les infrastructures de l'entreprise, le personnel et les éléments matériels et informels de ses activités.
- Pour cela, les moyens technologiques permettent de mettre en place un dispositif de surveillance et de protection des points sensibles et stratégiques.
- A cela, s'ajoute la parfaite connaissance du personnel.
- Et lorsqu'il s'agit de faire appel à des services extérieurs de manière ponctuelle ou régulière, la vigilance est alors l'affaire de tous les employés, à tous les niveaux, pour éviter toute effraction, tout vol de document ou de matériel.

Les employés dont les capacités d'action sont fixées en parfaite concordance avec la direction, doivent également témoigner de vigilance et de prudence dans les relations externes, avec le souci permanent de recouper l'information et d'éviter tout risque de fuite et de récupération de données capitales.

Eric Chatran mit fin à cette situation en se rendant à son tour sur le blog de l'informaticien de *Ventili*, constatant ainsi la gravité de l'affaire. Jacques Letourneur, convoqué le lendemain par Pierre Darmond fut informé des risques qu'il faisait courir à l'entreprise. Profondément affecté par ce qu'il avait provoqué, il mit fin à son blog.

5) Apparus à la fin des années 1990, les blogs connaissent désormais une forte intensité. Au point que l'on parle même de blogosphère.

« Points Clefs Formation »

Exposé au double-jeu

Si vous établissez un échange régulier avec un mystérieux interlocuteur, faites attention qu'il ne vous incite pas, au fur et à mesure, à dévoiler peu à peu des pans entiers des activités de votre entreprise. De sympathiques messages échangés ou même quelques rencontres amicales peuvent vous tromper sur les réelles intentions de votre correspondant.

Contacts multiples

Malgré tout, quelques cadres de *Ventili* firent preuve d'une imprudence comparable, durant une semaine, alors que certains d'entre eux étaient en déplacement à l'étranger.

Par souci de célérité, ils travaillaient à plusieurs sur les mêmes documents. Grâce à des logiciels de conception et de mise à jour dynamique de sites web [6], ils rendaient possible un véritable travail collectif. Ce qui les amena à mettre en ligne le contenu de documents importants, accessibles sur le portail internet de *Ventili* par mot-clé. Le tout conforté par des échanges de mails. Ils se concertaient notamment sur les améliorations à apporter à un nouveau modèle de ventilateur véritablement performant et sans égal sur le marché. Or, leur démarche attira l'attention de groupes de veille informatique concurrents. Et qui se firent un malin plaisir d'intercepter et court-circuiter le programme des cadres de *Ventili*. Les échanges de mails permirent ainsi de dévoiler le nouveau projet de *Ventili*…

Annie Baral, responsable de la Communication, s'en rendit compte lorsqu'elle reçut, quelques semaines plus tard, divers appels téléphoniques lui demandant des informations sur le nouveau ventilateur de *Ventili*. Or, théoriquement, le projet était encore confidentiel et Annie Baral n'avait en aucune manière lancé une campagne de promotion. En quelques jours, la cause de ces indiscrétions fut découverte, provoquant la colère de tous ceux qui, au sein même de l'entreprise, s'appliquaient à ne rien divulguer sur le projet.

6) Cela est possible grâce aux systèmes de gestion de contenu ou SGC (en anglais Content Management System ou CMS). La majorité des systèmes CMS offre la possibilité de catégoriser l'information, de l'indexer, d'utiliser des taxonomies, pour encore améliorer les méthodes de recherche. On peut donc créer des catégories de contenus, des sections (ou rubriques) voire des mots clés favorisant l'indexation.

« Points Clefs Formation »

La faille informatique :
entre correspondants mal attentionnés et interception des informations

Avec l'explosion des sources d'information par Internet, ce sont autant de risques d'être infiltrés. La vulnérabilité des systèmes internes de l'entreprise ne doit donc pas être minimisée – le risque zéro n'existe pas !

Il faut sensibiliser le personnel et faire appliquer des règles simples, entre autodiscipline et rigueur professionnelle. Car les risques se sont sensiblement élargis avec la multiplication des outils nomades : téléphones mobiles, pda, ordinateurs portables. Les interceptions d'informations, le pillage des données confidentielles de votre ordinateur sont courants. Le risque est d'autant plus élevé via les réseaux Wi-Fi, Wi-Max, liaisons Bluetooth, postes nomades. Le fait d'avoir des collaborateurs équipés de moyens mobiles de présentation et de communication (ordinateurs portables, téléphones mobiles avec Wi-Fi, assistants) doit donc être scrupuleusement pris en compte. Cela implique des précautions supplémentaires.

L'échange par Internet des données importantes avec des clients ou prospecteurs (gestion de commande, appel d'offre, etc) par mails, transferts de fichiers, connexions extranet sont autant d'opérations périlleuses, à moins de disposer de lignes sécurisées. A l'intérieur comme à l'extérieur de l'entreprise.

La onzième étude annuelle publiée en 2006, du Computer Security Institute (CSI), menée auprès de 600 entreprises américaines et accompagnée par le FBI, souligne que 75 % des pertes financières des entreprises américaines seraient dues au cybercrime.

Virus et vol de données

David Brissard, directeur du Service informatique de *Ventili*, était très fier de son parc informatique. Le matériel était performant, les postes confortables. Le personnel administratif et du département Recherche/Conception était satisfait. Un système intranet démontrait également sa parfaite utilité. Seul imprévu de taille pour David Brissard : l'intrusion de virus depuis le poste internet.

Tout fut provoqué par un mail anodin qui, en fait, cachait un virus. Une fois ouvert, le mail libéra le virus qui contamina tout le système informatique. Au point de le rendre inopérant. Plus aucune démarche ne pouvait être effectuée. Les postes informatiques étaient inutilisables.

David Brissard exprima sa surprise auprès d'Eric Chatran qui lui répondit qu'il avait eu le tort de mésestimer les potentielles attaques de virus informatiques et de ne pas avoir remis à jour les programmes de protection. En effet, David Brissard, par souci d'économie, n'avait pas cru bon de renouveler les mises à jour des anti-virus en dotation dans l'entreprise. Si bien que la protection était devenue bien fragile face à des virus sans cesse renouvelés et de plus en plus dévastateurs. Il regretta amèrement son choix. En effet, cela entraîna des coûts d'immobilisation pour l'entreprise, en raison de la paralysie des services informatiques. Cela se répercuta sur les activités mêmes de production et de distribution de l'entreprise. Tout fonctionnait au ralenti. Ce à quoi s'ajoutèrent les coûts de restauration des systèmes et de récupérations des données. Il fallut découvrir la nature même et la source de l'attaque informatique. Quel était le type virus concerné ? Quels dégâts avait-t-il causés ? Avec quelles conséquences ? Peut-on reconstituer le système informatique de l'entreprise ? Une attaque tardivement identifiée peut provoquer une mise hors service de l'entreprise de quelques heures à plusieurs mois selon la gravité.

Au final, *Ventili* dut payer une lourde facture pour remettre en service son parc informatique. Sans compter les pertes commerciales provoquées par l'interruption de la gestion des commandes.

« Points Clefs Formation »

Le poids des menaces informatiques

Les dégâts causés par des virus informatiques peuvent être considérables. Ils peuvent être évités grâce à une remise à jour permanente des programmes de protection informatique, et une bonne maintenance desdits systèmes.

La diversité des risques et des systèmes d'information fait que vous devez donc concevoir votre politique de protection de la manière la plus adaptée à votre propre fonctionnement. Ainsi, par exemple, si vous conservez sur vos systèmes informatiques des données confidentielles d'importance stratégique, vous devez naturellement en assurer la protection ; même si le risque zéro n'existe pas. Il y a toujours risque d'une faille dans vos procédures de protection. Il vous faut juste la réduire au maximum.

Sinon, les conséquences d'une « contamination » sont clairement identifiées. On distinguera notamment la perte d'informations et de données, d'où une perte de temps cruciale lorsque des clients attendent leurs livraisons. Qui n'a pas connaissance d'une entreprise dont le système informatique a été bloqué près de deux semaines en raison d'un virus informatique ? Au point qu'il faut

quasiment changer ou remodeler en profondeur tous les programmes et reconfigurer les pôles centraux. Ainsi, en 2003, près de la moitié des entreprises françaises ont été touchées par des virus et plus de la moitié d'entre elles – soit environ 25% – ont dû cesser leurs activités professionnelles au moins plusieurs heures, en raison de pertes de données.

Cela a nécessairement un coût direct, en raison de l'intervention d'une société d'informatique spécialisée. Il faut en effet des experts pour procéder au remplacement possible du disque dur d'un ordinateur, « purger » la centrale informatique de l'entreprise, réinstaller des programmes, etc.

On peut aisément imaginer les conséquences sur les autres domaines-clés de l'entreprise (renouvellement des moyens de production, réduction de l'obsolescence, politique salariale), en raison des retards de livraison des marchandises. Des retards qui, en chaîne, peuvent bloquer d'autres structures de production /distribution ou des chantiers.

En découlent une perte d'image de marque, une possible mise en cause sur le plan légal. Sans compter la remise en question des assurances générales de perte d'activité ou liées aux conséquences de telles attaques virales. On imagine par ailleurs aisément les pertes de clientèle qui, dans la plupart des cas, n'attend pas le retour à la normale et s'équipe auprès d'un concurrent.

Il est donc préférable, pour l'entreprise, de procéder de matière préventive plutôt que curative. Or, les études récentes montrent que les entreprises s'équipent de systèmes de protection performants seulement après avoir subi des attaques virales.

En France, selon les chiffres établis en 2002-2003 plus de 85% des entreprises victimes de sinistres de leur système informatique, absorbent elles-mêmes les conséquences financières avec leur propre trésorerie générale.

Pour éviter le pire

Le progrès continu des nouvelles technologies, ces dernières années, conforte Pierre Darmond et David Brissard, directeur du Service informatique, de mettre l'accent sur la protection de l'outil informatique. Ils dotent alors les divers ordinateurs de systèmes de sauvegarde et de sécurité à différents niveaux. Ceci afin d'éviter l'interception de données confidentielles. En outre, ils mettent l'accès aux ordinateurs sous accréditation. Seuls les utilisateurs clairement identifiés et dotés d'un code d'accès prédéfini peuvent travailler sur les postes informatiques. Ce qui limite d'autant les risques de fuites d'informations.

La protection des données contre une attaque informatique exige la mise à jour perpétuelle des systèmes de protection informatiques. Elle va nécessairement de pair avec un personnel compétent, fin connaisseur et sensibilisés à l'importance de la protection des données dites confidentielles.

« Points Clefs Formation »

Avantages et limites du télétravail

La mutation des outils de travail va de pair avec le marché du travail lui-même qui voit s'amplifier le recours au télétravail. Considéré comme avantageux pour les entreprises, il permet de ne pas renforcer le nombre de salariés permanents, et plutôt de solliciter des contractuels. Mais ce type d'activités présente aussi des inconvénients.

En multipliant les contractuels, la direction de l'entreprise accentue les prises de risques, les fuites éventuelles d'informations ou même leur interception. Les collaborateurs extérieurs, en travaillant à distance sont amenés à se connecter au système interne de l'entreprise, d'où une ouverture de risque en mettant en péril la confidentialité de données.

En 2004, la moitié des collaborateurs d'entreprises françaises travaillaient avec des mots de passe et 35 % d'entre eux les communiquaient à un tiers.

La tentation de charger des logiciels sur Internet

Vous pouvez être tenté d'utiliser des logiciels dits libres. Des programmes facilement accessibles sur l'Internet et que vous allez charger sur votre ordinateur. Ils sont attractifs car ils proposent divers types d'application de la gestion de production à la gestion d'achats, des questions logistiques à la gestion du personnel. Leur utilisation et modification ne nécessitent aucune licence d'utilisation. Citons comme exemples les programmes OFBiz, Value, Sugar CRM ou ERP5.

Qu'est-ce qu'un spyware ?

Le spyware est un programme informatique espion qui se charge dans la plus grande discrétion. Il ne peut être contré que par un système anti-virus performant, mis à jour régulièrement.

Selon des études récentes, 87% des ordinateurs des entreprises sont infectés par des spywares. De même, avec le programme Rbot-GR, il est possible d'être espionné depuis la webcam d'un PC.

L'efficacité de ces divers systèmes est redoutable, surtout lorsque l'on sait que 60 % des entreprises ignorent après coup qu'elles ont été la cible d'attaques particulières.

Eric Chatran, en accord avec la Direction, tenta de procéder à une pénétration du système informatique depuis l'extérieur pour s'assurer de la qualité de la protection du réseau. C'est avec un réel soulagement qu'il constata la qualité du système de sécurité au terme de plusieurs tentatives de pénétration. En même temps, Eric Chatran sait combien tout système présente une faille qui peut être astucieusement exploitée par un pirate informatique, un hacker, fin spécialiste. Reste que pour l'essentiel, le parc informatique de *Ventili* était protégé contre les virus désignés « chevaux de Troie ». Ces programmes peuvent neutraliser les systèmes et surtout permettent au visiteur clandestin d'ouvrir vos fichiers et de prendre connaissance des contenus. Il lui est même possible de mener des attaques informatiques vers d'autres sociétés en utilisant vos propres systèmes ce qui vous place dans une situation extrêmement délicate. Cette seule idée donne des sueurs froides à Pierre Darmond.

« Points Clefs Formation »

Vulnérabilité potentielle d'un ordinateur

Une fois connecté sur Internet, chaque ordinateur est identifié par un numéro unique (adresse IP). Chacun d'eux est donc susceptible de faire l'objet d'attaque ciblées, par le biais de virus.

L'installation d'un système de sécurité requiert les services d'une société informatique spécialisée, et fiable. A terme, il s'agit de bloquer toutes les attaques automatisées, réduire au maximum la prolifération des virus et détecter les intrusions dans les systèmes.

« Points Clefs Formation »

Les sauvegardes : une mesure impérative

Le processus de sauvegarde doit être systématique. Cela permet de récupérer toutes vos données, lorsque votre système est corrompu ou que vous avez perdu des informations à cause d'un virus.

Le principe de sauvegarde peut être fastidieux. Mais il fait toute la différence en cas de grave problème informatique. Il permet une reprise plus rapide des activités de l'entreprise.

On ne soulignera jamais assez la pertinence de la garantie d'un service de maintenance de vos capacités de défense informatique. Si les capacités financières de l'entreprise le permettent, il peut être opportun de disposer de son propre service de maintenance.

Mais les principes élémentaires de protection des systèmes relèvent aussi des gestes quasi automatiques dont le coût est somme toute des plus réduits : mises à jour de sécurité de votre système d'exploitation via Internet par exemple ; configuration d'anti-spam, de pare-feu de qualité pour un montant réduit mais cyclique et récurrent. En moyenne, les mises à jour se font toutes les semaines, notamment lorsqu'il s'agit des antivirus, es correctifs de logiciels de sécurité. Pour les versions de moteur antivirus, le contrôle de vulnérabilité ou non, l'application des politiques de sécurité, les configurations de firewalls, les mises à jour s'effectuent tous les trimestres. La situation est plus complexe lorsque vous souhaitez doter votre système d'un niveau d'authentification pour filtrer l'accès à des données et informations dites sensibles.

L'importance des antivirus

En 2003-2004, quelques 4 240 883 évaluations pratiquées par les instances spécialisées sur les capacités de sécurité informatique des entreprises, ont révélé que 19 % des sites informatiques étaient vulnérables faute de mises à jour régulières. Ce qui les exposait à des attaques qui avaient 100% de chances d'aboutir. Chaque ordinateur doit être doté d'un pare-feu ou firewall. Et l'on peut doubler la protection d'un pare-feu sur le périmètre externe comme sur l'ensemble du réseau.

L'atout technologique

Pierre Darmond fut confronté à un nouveau cas de fuites de données par le biais des outils technologiques d'ordre privé. Ainsi, une secrétaire de *Ventili* ne fut-elle démasquée qu'au bout de quelques semaines. Son comportement fut en effet jugé suspect non seulement pas ses collègues mais aussi parce qu'elle semblait passer plus de temps à utiliser son téléphone portable. En fait, après l'avoir soigneusement observé, et en recoupant les informations avec celles d'autre secrétaires, Eric Chatran constata que la secrétaire envoyait pas le biais de son téléphone portable le contenu des derniers contrats signés par *Ventili* avec des clients de pays sud méditerranéens. Elle avait même pris des photos des chaînes de montage avec son téléphone portable de nouvelle génération. Les informations parvenaient à son époux qui usait de ces atouts pour faire valoir les intérêts propres de son entreprise auprès de concurrents de *Ventili*. La secrétaire fut licenciée pour manquement au principe de discrétion professionnelle.

Peu après Pierre Darmond transmit de nouvelles directives à tous les employés et cadres en les priant de ne pas utiliser de téléphone portable ni de clé USB personnels dans les bureaux d'études ou au niveau des chaînes de production et d'assemblage de l'entreprise.

« Points Clefs Formation »

Un large éventail de matériel électronique

Téléphone portable, clé USB, téléphone numérique pour éventuellement récupérer des informations d'importance économique... Autant d'outils qui permettent le transfert d'informations. Mais aussi leur vol. On signalera la possibilité depuis un ordinateur portable de pirater les données (carnets d'adresse, SMS, photos, etc) de téléphones mobiles[7]. On a à noter aussi le système d'ondes radio, bluetooth, qui rend possible le lien sans fil d'un téléphone portable ou d'un PDA à une oreillette. Toute une gamme technologique, toute une liste de vulnérabilités informatiques qu'il est difficile de contrôler.

7) Un ordinateur portable équipé d'une antenne, d'un clé USB, d'un logiciel canner peut détecter touts les téléphones portables dans un rayon d'une quinzaine de mètres alentours. Le curieux peut y pénétrer et voler toutes les données qui s'y trouvent.

Un autre cas de figure conduisit Pierre Darmond à mettre en place un système de surveillance. Il voulait à tout prix en avoir le cœur net sur le comportement jugé suspect d'un technicien qui semblait communiquer avec l'extérieur depuis son ordinateur via l'internet.

Pour procéder d'une certaine manière à une traçabilité de la journée de travail de l'employé, la direction procéda à la mise en place d'agents informatique assimilés à de véritables mouchards virtuels ; à savoir les key loggers et les log trackers. Le key logger enregistra toutes les frappes effectuées sur l'ordinateur. Ce qui permit de suivre l'intégralité de la journée de travail du salarié. Le log tracker, pour sa part, suivit l'utilisation par l'employé du service internet, en répertoriant les divers sites et services visités et sollicités.

Ces mesures permirent de confondre le technicien qui était en contact régulier avec un concurrent de *Ventili*. A plusieurs reprises, il communiqua de la sorte des données techniques sur un nouveau projet de motorisation de ventilateur. Cette motorisation, sur le point d'aboutir, faisait partie des atouts dont voulait jouer *Ventili* pour étendre son marché.

Certes, Pierre Darmond put mettre fin au double jeu du technicien. Mais il ne pouvait le licencier car sa méthode pour le confondre était illégale.

« Points Clefs Formation »

Usage des key logger : attention aux dérives illégales !

Le recours aux key loggers et log trackers n'est autorisé que dans le cadre de statistiques globales. En aucun cas, il est permis de viser un employé particulier. Attention, par conséquent, de ne pas aller à l'encontre de la liberté individuelle, par excès de sécurisation ou de tentation de basculement dans le « tout contrôle ». D'autant plus que les key loggers permettent aussi et surtout d'enregistrer la frappe de mots de code ou de numéros de cartes bancaires…

Ces dernières années, la Justice traite de plus en plus de cas où des chefs d'entreprise ont outrepassé leurs droits en plaçant sous surveillance un ou une employée. La découverte, après espionnage du contenu d'un disque dur, d'éléments sans aucun lien avec le domaine professionnel sert trop souvent de leitmotiv pour procéder au licenciement de l'intéressé(e). On ne peut en effet cautionner de tels comportements humainement, éthiquement, répréhensibles. Pour autant, les textes juridiques n'interdissent pas clairement les contrôles. Ils doivent seulement être faits en connaissance de l'intéressé, non pas à son insu.

Ainsi, est-il toujours impératif d'agir en totale transparence vis-à-vis des employés. C'est d'ailleurs le principe même du bon fonctionnement d'une entreprise. En vertu d'une communication fluide, quasi naturelle entre les employés et la direction. Condition sine qua non pour établir un véritable lien de confiance et de coordination constructive autant que productive. Enfin, les moyens en surveillance mis en œuvre par la direction doivent être proportionnels à la réalité des risques encourus[8].

De même, il est opportun de pouvoir s'appuyer de manière assez dynamique – pour ne pas dire offensive – pour collecter des informations en vertu d'un pôle dit de veille informatique.

B) Assurer la veille informatique

S'il y a un bien un secteur déterminant en matière d'intelligence économique c'est assurément celui de la veille informatique. Elle se décline en plusieurs domaines complémentaires : veilles organisationnelle et réglementaire, politique et administrative, financière, concurrentielle et commerciale.

Le pôle de veille

Eric Chatran, à la demande de Pierre Darmond, mit en œuvre et pilota un dispositif de recueil, d'analyse et de diffusion de l'information. Parallèlement, il créa un système de mémorisation et de capitalisation des connaissances de *Ventili*. Ces données pratiques et techniques constituent en effet le patrimoine même de l'entreprise. Elles en assurent d'une certaine manière la pérennité sans que soient négligés des apports nouveaux. Elles doivent donc à tout prix être protégées.

Mise en place...

L'entreprise *Ventili* mise donc sur la création d'un pôle de veille informatique. Le Service de Gestion des ressources humaines, en corrélation avec la Direction et le pôle informatique, détachent à cet effet deux personnes. Les deux volontaires sont trouvés sans difficulté parmi les informaticiens de *Ventili*, jugés aptes à remplir cette mission de confiance et d'importance stratégique pour l'entreprise. Ils témoignent par ailleurs d'une solide

8) En 2005, une filiale de la SNCF était condamnée pour avoir mis en place un système de pointage de son personnel par empreinte biométrique ; une démarche jugée disproportionnée au regard de la réalité économique de l'entreprise incriminée.

expérience professionnelle au sein de *Ventili* et connaissent parfaitement le secteur des ventilateurs.

Afin de renforcer leurs capacités en matière de gestion et d'analyse des informations, la Direction leur assure un stage de formation en concertation avec l'Ecole de Guerre économique et la FéPIE, véritables pôles d'accompagnement et de formation pour les PME/PMI françaises.

...et fonctionnement

Au terme d'un stage d'une semaine environ, les deux informaticiens disposent, dans un bureau spécialement aménagé, de plusieurs unités centrales. Chacune d'elle est reliée à un moteur de recherche différent. Les moteurs de recherche retenus sont jugés comme les plus à même d'apporter les informations pertinentes.

En amont, avec Eric Chatran et Pierre Darmont, les deux informaticiens fixent une stratégie de sélection des mots-clés. Ils orientent ainsi la nature des informations qui doivent être retenues. Jour après jour, semaine après semaine, les informations collectées sont alors être triées, répertoriées. Elles sont sélectionnées à nouveau et résumées afin de dresser des bilans intermédiaires puis épisodiques. La quintessence en est transmise à la Direction, sous forme de dossiers synthétiques, tandis que les développements correspondants vont être classés par thème, par zone géographique, par degré d'importance.

Ainsi, le pôle de veille put-il archiver divers dossiers thématiques. Certains portent notamment sur la réalité du marché des ventilateurs en Afrique du Nord, d'autant plus à l'heure de la mise en avant des liens euro-méditerranéens. Un autre fait le point sur la concurrence en Europe de l'ouest ; un autre sur l'évolution climatique dans les pays de l'hémisphère nord ; sur les habitudes de consommation en matière de rafraîchissement d'air/air conditionné des populations occidentales, etc.

Exploitation des informations

En toute logique, le secteur de la ventilation a des prolongements d'études sociologiques, pour connaître les coutumes et habitudes de consommation. Sur un plan plus technique et conceptuel, la veille permet également de collecter toutes les informations portant sur le ventilateur en tant que tel ; bien utilitaire qui bénéficie à son niveau des progrès technologiques, de l'évolution d'une motorisation de plus en plus silencieuse, avec une étude des diverses ergonomies, des styles les plus en vue selon les aires culturelles visées. En soit, un ventilateur destiné au marché français n'aura pas les mêmes caractéristiques qu'un ventilateur destiné au marché asiatique par exemple ; marché d'autant plus difficile à percer qu'il est justement fortement soumis à la mainmise des producteurs asiatiques.

Tout en procédant au recueil et au classement des informations inhérentes au secteur d'activité précité, les responsables de la veille informatique, sous la conduite d'Eric Chatran, sont aussi attentifs à l'évolution même des outils électroniques et technologiques. Autant d'instruments à leur disposition, qui facilitent leur tâche quotidienne. Ainsi, met-on par exemple de plus en plus en avant l'utilisation des flux RSS blogs [9] qui permettent aux entreprises de mettre en œuvre de nouvelles stratégies d'information de veille et de micro-marketing. Une démarche qui s'inscrit dans les nouvelles approches du management.

« Points Clefs Formation »

Il existe même des programmes informatiques associés à des moteurs de recherche performant qui vous permettent de réaliser des requêtes afin de découvrir, par catégories référencées, par disciplines, par zone et espace géographique, les pôles d'intérêt pour votre politique d'entreprise. Cela est d'autant plus porteur que les PME et PMI sont plus sensibles à leur environnement que les grandes entreprises.

Quant à la possibilité de quantifier la valeur économique d'une information ou, à l'inverse, son absence, cela reste quasi impossible. Mais il est possible de mettre en place un système de pilotage de l'IE en procédant à un audit, une évaluation et au contrôle qui, au final, permettent d'apporter quelques corrections.

Evolution permanente du pôle

Une fois le secteur de veille informatique devenu opérationnel, Eric Chatran n'a de cesse de réfléchir à l'élargissement du potentiel du service. Et peu à peu, il devient nécessaire de doubler l'équipe de veille deux hommes (qui seront deux femmes sous la conduite d'Eric Chatran). En même temps, il faut prévoir l'évolution professionnelle des personnes déléguées pour ce secteur. En effet, il faut anticiper d'éventuels départs plus ou moins longs, au gré de congés de maternité, de démissions ou de réorientation professionnelle des intéressés. Autant de cas particulier qui implique de la part de la direction de

9) Un flux RSS ou fil RSS ("RSS Feed" en anglais pour Really Simple Syndication (syndication vraiment simple), ou de Rich Site Summary (Sommaire d'un site enrichi) est un format de contenu Web avec une mise à jour permanente du contenu. Cela est particumièment fréquent sur les sites d'informations ou sur les blogs professionnels ou semi-professionnels.

l'entreprise, réactivité et prévision de surseoir au poste susceptible d'être vacant. Le but, on l'aura compris, étant d'assurer la permanence du service de veille. Ce qui implique en parallèle une réelle communication et harmonie des personnes en charge du secteur avant leur départ au profit de leurs successeurs – définitifs ou temporaires – afin que les méthodes appliquées soient préservées, tout comme la gestion des résultats et leur finalité.

Si l'attention, on l'a vue, se porte avec rigueur sur la collecte d'informations, le recueil de renseignement, le suivi de l'évolution du marché depuis les postes informatiques, en surfant sur la Toile, il faut par ailleurs être attentif aux démarches qui peuvent être remplies à l'extérieur même des infrastructures de l'entreprise.

« Points Clefs Formation »

L'outil informatique est tout autant un formidable outil professionnel qu'un « Talon d'Achille ».

Il exige compétence et professionnalisme, doublés de rigueur et d'attention permanente pour savoir l'utiliser dans toutes les dimensions.

Les progrès technologiques en font un moyen de communication et de stockage d'informations en perpétuelle évolution et transformation. D'où la nécessité de se tenir au courant de toutes les nouveautés techniques, des programmes performants. Et de réfléchir aux solutions optimales pour, sans cesse, améliorer les capacités du parc informatique.

En même temps, il s'agit d'être vigilant face aux tentatives d'infiltration frauduleuses et malintentionnées.

Véritables points faibles dans l'entreprise, les ordinateurs, reliés à l'extérieur par internet, peuvent être l'objet d'attaques de concurrents sous forme de virus informatiques et une véritable plate-forme pour le pillage de vos informations confidentielles.

En conséquence, il faut s'assurer de la sauvegarde régulière des fichiers informatiques et veiller à la mise à jour et au renouvellement des programmes antivirus.

4) Gérer l'information et la communication

Pour l'efficacité de son entreprise, Pierre Darmond considère qu'i faut à la fois gérer la communication interne et maîtriser les flux d'informations extérieures. Ces dernières se composent des éléments essentiels, susceptibles d'être utiles dans le domaine d'activités de *Ventili*. Il faut être réellement à l'écoute de son environnement concurrentiel afin de bien s'en imprégner, le comprendre et s'y adapter. C'est pourquoi la culture de Veille dite stratégique au sein de l'entreprise a toute son importance. Pour *Ventili*, il s'agit de suivre de près l'évolution technologique en matière de ventilation, non seulement dans les pays anglo-saxons mais aussi asiatiques. Quelles sont les matières de plus en plus utilisées ? Quels types de moteurs à la fois résistants et silencieux arrivent sur le marché ? Quelles sont les règles européennes au niveau de la sécurité du consommateur ? Quelles sont les analyses faites quant à l'évolution du marché, des modes d'utilisation à caractère privé ou professionnel ? Faut-il privilégier la ventilation sur pied ou avec fixation murale ? Autant de thématiques que le service de veille doit prendre en compte pour rassembler le maximum d'informations pertinentes.

« Points Clefs Formation »

Tout repose donc sur des notions clés telles que veille concurrentielle et stratégique, intelligence compétitive, culture d'entreprise, communication interne.

La veille concurrentielle est d'autant plus importante que près de 70% des salariés de PME/PMI déclarent ne pas connaître ou méconnaître la concurrence.

Compte tenu de l'évolution du marché, *Ventili*, au gré des NTIC, s'applique à faire évoluer son périmètre d'activités en évaluant la faisabilité d'acquisitions. Elle envisage même des alliances stratégiques avec des partenaires publics ou privés, notamment en matière de Contrats Recherche et Développement, d'ingénierie, de brevets et de licences. Mais, finalement, après mûres réflexions, Pierre Darmond renonce à de tels cas de figure. Il préfère rester indépendant et s'en tenir à sa propre politique d'entreprise.

De surcroît, *Ventili* met en valeur un référentiel à la fois précis et porteur, qui lui permet de faire des choix stratégiques. Il faut donc prendre en compte les critères juridiques, commerciaux, technologiques, géopolitiques, de marketing, réglementaires et concurrentiels de son domaine d'activités.

« Points Clefs Formation »

Composantes de l'intelligence économique

- Veille concurrentielle, commerciale ;
- Veille géopolitique ;
- Veille technologique, brevet, veille réglementaire ;
- Veille sociétale

La veille concurrentielle permet de mieux connaître les concurrents, de cerner leurs démarches commerciales, leur logique entrepreneuriale, leur marketing (techniques de vente, de distribution) parfois leurs résultats et leurs perspectives.

La gestion de l'information est donc essentielle pour le fonctionnement de *Ventili*. Et l'intelligence économique est logiquement attachée à la politique de l'entreprise en matière de maîtrise de l'information, ainsi qu'aux stratégies de surveillance des environnements.

A) Organiser et protéger l'information

Depuis les années 1990, *Ventili*, née à la fin des années 1970, est de plus en plus confrontée à la nécessité de gérer une masse croissante d'informations. D'ailleurs, pour un quart des salariés, il y a surinformation et donc incapacité, en retour, à gérer et absorber cette information.

Pourtant, on l'a vu, ces informations sont nécessaires puisqu'elles contribuent à une meilleure perception de l'environnement socio-économique de l'entreprise. Le principe de veille traduit donc cet effort permanent de gestion de l'information. Ne sont conservées que les informations utiles. De la sorte, la veille stratégique perçoit l'information comme un outil d'anticipation

et de développement technologique. Elle permet de bien suivre l'évolution du marché international de la ventilation.

« Points Clefs Formation »

Il existe trois catégories majeures d'informations

Elles s'inscrivent entre intelligence économique et espionnage industriel :

- L'information dite « blanche »

Librement accessible, elle représente environ 80% de l'information intégrée à une logique de veille. Par contre, elle est généralement peu stratégique ;

- L'information dite « grise »

Il est plus difficile d'y accéder. De même il n'est pas évident de la valider. Principal atout, son caractère d'anticipation. Elle constitue 15% de l'ensemble et focalise l'attention des « veilleurs » ;

- L'information dite « noire »

Il s'agit de l'information protégée, confidentielle, avec une diffusion restreinte (5 % de l'ensemble des informations). Elle concerne essentiellement les secteurs stratégiques de l'Etat. En disposer résulte d'une action illégale.

Comme l'information, la politique de veille intègre elle aussi plusieurs niveaux.

« Points Clefs Formation »

Les divers niveaux de veille

- Veille ponctuelle.
- Veille occasionnelle.
- Veille systématique ou périodique.

Chez *Ventili*, les responsables du pôle de veille tiennent des fichiers dans lesquels figurent les noms des personnes qui apportent les informations.

Mais pour certains acteurs témoins de la vie de l'entreprise, la notion d'information est à tort associée au pouvoir. Au même titre que la compétence.

Pierre Darmond a donc lancé une véritable campagne de sensibilisation du personnel pour rassurer, et s'inscrire dans une démarche pédagogique. Les doutes et malentendus se sont alors évanouis et désormais toute l'entreprise *Ventili* travaille sereinement sans a priori vis-à-vis de la direction avec laquelle le dialogue est permanent et toujours constructif.

Il faut aussi veiller à une bonne diffusion une bonne circulation de l'information. En évitant que les niveaux hiérarchiques intermédiaires ne la conservent, la court-circuitent ou la réorientent de manière arbitraire. Car le partage de l'information est essentiel pour le bon fonctionnement de l'entreprise. Il contribue tout simplement au respect du caractère collectif du travail entrepris.

En même temps, il faut que chacun soit convaincu de contribuer à la veille et à la collecte d'informations. De même, la direction, qui reste quand même l'élément d'impulsion de la démarche collective, doit-elle être convaincue de l'utilité de la politique menée.

En dépit des risques concurrentiels, le chef d'entreprise de *Ventili* a mis longtemps avant d'intégrer les risques d'attaque et de pénétration du système d'information par des opérateurs mal intentionnés. Après avoir constaté une fuite quant à un projet de pénétration du marché sud-méditerranéen, ce qui lui valut une perte de marchés potentiels, il a fini par admettre la nécessité de consolider un service approprié pour faire face à de tels cas de figure.

« Points Clefs Formation »

La mise en place d'un pôle de veille informatique

La direction de l'entreprise doit pouvoir compter sur la connaissance technique des experts et, surtout, disposer des capacités financières requises pour créer, développer et optimiser un tel service. Car, de façon quasi permanente, il faut ensuite adapter voire remodeler cette structure en tenant compte de l'évolution de l'intelligence économique. Par la même, il faut savoir se remettre en cause en sachant toujours dresser un bilan avec les erreurs, les besoins de réorientations, les améliorations pouvant être apportées, etc.

Il faut bien réaliser à quel point l'entreprise – comme n'importe quel citoyen finalement – évolue dans un contexte marqué par le flux continuel d'informations, sachant que les flux d'informations créées doublent en volume tous les quatre ans.

Ce qui exige, en retour, une organisation rationnelle pour la gérer sinon la canaliser et, si besoin, l'exploiter de manière précise pour en tirer profit.

L'entreprise doit s'adapter au nouveau contexte et favoriser sa fonction

■■■ Renseignement en reposant sur les systèmes binaires et complémentaires dans ce secteur : technique/humain, science/culture, quantité/qualité, concurrence /coopération. Aussi, le pôle Renseignement doit-il contribuer largement à la prise de décision en fonction des informations réunies et exploitées.

L'information, de toute évidence, est au cœur de l'intelligence économique (IE). L'entreprise doit donc consolider sa propre culture de l'information en favorisant la mise en commun des informations.

Il est d'ailleurs possible d'identifier les principales sources d'information [10] : les catalogues des concurrents ; les études techniques des ventilateurs les plus en pointe ; le suivi des divers brevets identifiés ; l'évolution des méthodes de production notamment dans les pays anglo-saxons, etc.

De manière plus précise, on peut même distinguer les informations formelles et informelles, comme en témoignent les tableaux suivants :

SOURCES	AVANTAGES	INCONVENIENTS
Presse	- Spécialisée ; - Grand public ; - Information.	- Sélection, plus ou moins fastidieuse ; - Informations publiées considérés comme déjà « mortes » (dépassées).
Ouvrages	- Synthèses denses d'informations.	- Profusion des publications ; - Informations rapidement obsolètes.
Banques de données informatisées	- Exhaustivité, facilité d'accès ; - Faible coût des recherches.	- Nécessité de recouper l'information pour la valider ; - Peu de documents originaux.
Brevets	- Contiennent près de 80 % des informations techniques.	- Compréhension parfois difficile ; - Nécessité de traduire diverses langues étrangères ; - Certains secteurs non couverts.
Sources d'informations légales	- Facilité d'accès.	- Caractère restrictif ou limité de ces informations.
Etudes prestataires	- Informations de qualité.	- Coût important.

10) Rapport du Club informatique des grandes Entreprises françaises (CIGREF), « Intelligence économique. Les systèmes d'information au cœur de la démarche », mai 2003.

SOURCES	AVANTAGES	INCONVENIENTS
Concurrents	- Informations disponibles par le canal de la presse interne, par le biais de leurs communications commerciales et financières et lors des Journées portes ouvertes.	- Difficultés de s'assurer de leur crédibilité ou validité ; - Accès de difficulté variable.
Fournisseurs et sous-traitants	- Possibilité d'étoffer et valider des informations obtenues par d'autres canaux.	- Inscription dans le jeu des concurrents.
Banques de données informatisées	- Exhaustivité, facilité d'accès ; - Faible coût des recherches.	- Peu d'éléments décisifs ou d'aide à la décision.
Missions, voyages d'études	- Sources riches d'informations.	- Caractère onéreux de la démarche.

Il faut donc, au gré de la collecte d'informations, être capable de sélectionner les éléments intéressants qui peuvent jouer sur la prise de décision et sur la stratégie de l'entreprise. L'information utile peut aussi intégrer des données capitales, de nature quasi vitales pour la prise de décisions. C'est donc cette forme d'information que la veille stratégique va tenter de capter en priorité.

« Points Clefs Formation »

Buts et objectifs de la collecte d'informations

Il s'agit pour l'entreprise d'assurer systématiquement la recherche et l'exploitation de l'information, au même titre que la protection et la défense du patrimoine immatériel. Autant d'impératifs qui doivent tenir compte de l'environnement national et international, dans un contexte de compétitivité, avec les enjeux économiques que cela comporte.

- **Pourquoi ?** Définir clairement les objectifs recherchés en fonction des enjeux eux aussi précisément identifiés ;

- **Quelles informations (Quoi) ?** Quelles sont les informations à privilégier ?
- **Par qui ?** Quelles sont les personnes chargées de réaliser ces recherches ?
- **Quand ?** Sur quelle durée, à quel rythme, selon quelle fréquence ?
- **Comment ?** Quels sont les moyens requis pour remplir ces démarches ?
- **Où ?** Quelles sont les zones géographiques ou les sources précises à privilégier et auxquelles se limitent les recherches ?
- **Combien ?** Quel est le budget de l'entreprise alloué ou prévisionnel pour ce type d'activité ?

La propriété intellectuelle

Au même titre qu'un ouvrage, un brevet, un dessin, un modèle ou un programme informatique relève du principe de la propriété intellectuelle. Or, aujourd'hui, les entreprises évoluent dans un contexte où les cas de violation de la propriété intellectuelle, les falsifications sont de plus en plus fréquentes. Le dépôt de brevet, par exemple, doit répondre à une stratégie de préservation de la raison d'être même de l'entreprise qui en dispose, afin d'éviter d'être copiée et pillée.

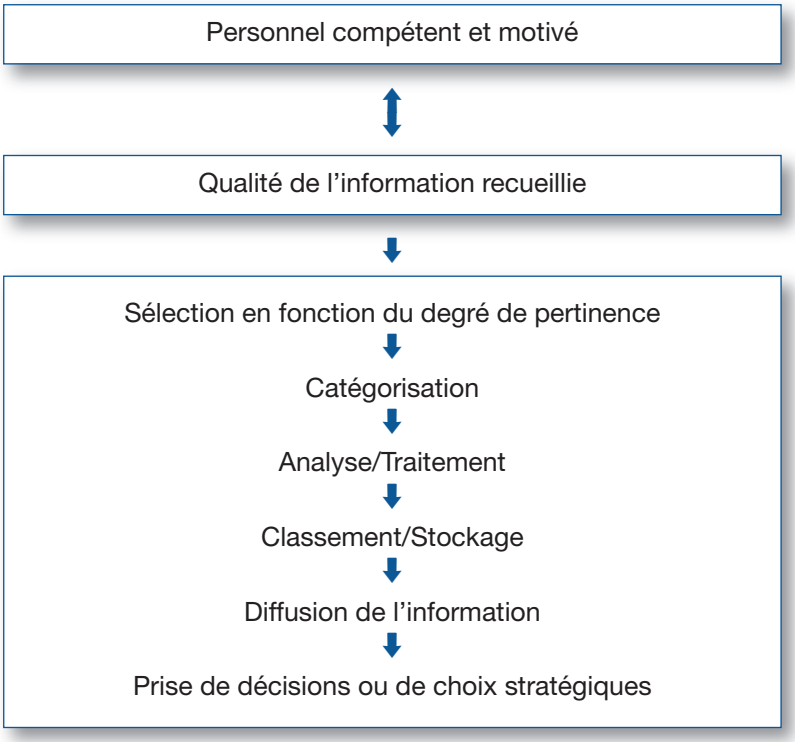
Il est impératif pour *Ventili* de s'assurer du dépôt de ses brevets de manière rigoureuse, pour les protéger contre les prédations. A titre d'exemple, il peut y avoir tentative de détournement de brevet.

C'est ce qui arriva lorsqu'un ingénieur de *Ventili*, après plusieurs mois de travail, réussit à mettre au point un ventilateur doté d'une motorisation ultra silencieuse. De surcroît, les capacités de ventilation de l'appareil étaient particulièrement performantes. Or, avant que la direction de *Ventili* procède au dépôt du brevet, l'ingénieur n'hésita pas à contacter un puissant concurrent pour lui vendre sa création. Finalement, cela ne se fit pas. Le concurrent, à la fois scrupuleux et hésitant, ne donna pas suite.

Hiérarchiser l'information

On l'a dit, il faut aussi savoir préserver la qualité – plutôt que la quantité – des informations recueillies. Ce qui implique une classification méthodique en fonction de ce que l'on recherche, des priorités que l'on se donne.

Il faut donc relever des défis techniques permettant à la fois de brasser mais surtout cibler la masse d'informations prioritaires ; informations qui, dans le même temps, doivent donc être protégées.



Si, d'un côté, le recueil de l'information et son analyse sont précieuses, il faut savoir aussi la protéger en l'intégrant dans une politique de sécurité des organisations de l'entreprise. Autant que possible, il faut en effet éviter toute compromission, altération ou disparition de l'information ou des connaissances. La société *Ventili* est aussi sensible à ce que la veille concurrentielle, par exemple, se fasse vite et soit simple en matière de procédure.

L'entreprise *Ventili*, à tous les niveaux, a bien intégré la notion de diffusion de l'information et de communication interne. Mais seuls 25% des employés, tous services confondus, ont le réflexe du support papier ; les autres stockent leurs données sur leur ordinateur. Ce qui est bien entendu un réflexe de célérité et de simplicité dans la démarche. Mais, cela exige aussi une méthode de contrôle de la fiabilité des mesures de sécurité et du degré de vulnérabilité du système d'information. On l'a vu, Eric Chatran peut procéder lui-même à des tests de fiabilité. Mais il est aussi possible d'effectuer un audit de sécurité pour mesurer la fiabilité de la protection établie. On peut alors apporter des modifications afin de rendre les mesures de sécurité des systèmes plus performantes.

« Points Clefs Formation »

L'information : élément-clé de l'intelligence économique

Pour valider l'information recueillie, il faut utiliser des techniques d'évaluation, des grilles de validation, et des recoupements, pour être certain que l'information visée est fiable. Cette démarche de validation - en fonction de l'analyse et de la corrélation des éléments d'information - s'inscrit donc dans une logique d'entreprise. Tout s'intègre dans une problématique en vertu des stratégies prévues et applicables, entre prévision et prospective. Compte tenu du caractère aléatoire de certaines informations ou des changements observés, il faut aussi être capable de réactivité et d'adaptation collective, pour coller à la conjoncture. Le tout en sachant s'appuyer sur l'atout des technologies de l'information et de la communication, élément récurrent sur lesquels se base l'intelligence économique.

En dehors des systèmes fixes à l'entreprise, il est aussi des outils individuels qui contiennent des informations importantes, voire parfois capitales.

B) Emploi du temps, PDA et téléphonie mobile : les limites

Les nouvelles technologies facilitent la gestion quotidienne des emplois du temps et des informations professionnelles. Leur vulnérabilité n'en est que plus importante.

« Points Clefs Formation »

Au quotidien, vous façonnez votre emploi du temps, établissez des prévisions, prenez des rendez-vous. Autant d'activités complémentaires qui sont, par définition, l'objet de toute l'attention d'une concurrence déloyale. En toute logique, vous avez largement recours aux nouveaux moyens des NTIC dont nous avons déjà parlé. Ce à quoi s'ajoute l'assistant personnel numérique ou PDA pour Personal Digital Assistant.

Interception et pillage de données quasi confidentielles

Ce petit appareil numérique portable est en effet aujourd'hui omniprésent dans la vie active. Il prend peu de place, grâce à sa taille réduite, comparable à celle d'une calculatrice [11]. Il offre une multitude de possibilités (agenda, répertoire téléphonique, bloc-notes) avec un clavier incorporé et un style qui permet d'intervenir directement sur l'écran tactile. Les nouvelles générations de PDA peuvent recevoir des outils multimédias (vidéo, images) en du téléphone. Le PDA, qui dispose déjà d'une mémoire confortable, peut aussi prendre en compte une carte-mémoire qui augmente encore ses capacités de mémorisation de données (avec des cartes de 512 Mo à 4-8 GO).

Les PDA sont désormais dotés de liaisons WiFi ou Bluetooth. Ce qui les rend, dans ce cas, comparables à des téléphones mobiles. Si bien qu'un cadre commercial de *Ventili* en déplacement, peut être mis sur écoute, non seulement via son téléphone mobile mais aussi par le biais de son PDA. Il peut alors devenir la cible de procédures de pillage des informations enregistrées dans ses moyens de communication mobiles.

On le voit, tous ces outils technologiques capables d'une forte mémorisation de données, sont des cibles privilégiées pour de potentiels voleurs ou concurrents sans scrupule. Rappelons-nous l'exemple de l'interception de données par un spécialiste à côté de vous, dans un transport en commun ou un lieu public. Il faudra donc plutôt stocker les données dans un endroit sûr, faire des copies sur CD, par exemple, soigneusement conservées dans l'entreprise.

« Points Clefs Formation »

Savoir face à une situation de crise

A tous les niveaux il faut aussi prévoir des situations de crises. De la prévention à sa gestion, la crise est aussi une composante de la vie de l'entreprise. Il vaut donc mieux l'apprivoiser, la dompter, plutôt que l'ignorer par crainte ou par simple négligence, en estimant à tort que « cela n'arrive qu'aux autres ». Lorsque des informations vous sont volées ou sont altérées, le constat, tout d'abord, n'est pas nécessairement instantané. Vous pouvez mettre du temps à vous en rendre compte car les conséquences peuvent tarder à se faire sentir.

11) Le concept du PDA a été créé par la société Apple Computer au début des années 1990

De même, si vos systèmes de surveillance et de sécurisation ne sont pas actualisés, les infiltrations sont facilitées et d'autant plus lourdes de conséquences. Le bilan peut se révéler dramatique : copie du listing des fichiers clientèle, copies de données techniques de tous les ventilateurs produits par l'entreprise ; planification et perspectives d'ouverture de nouveaux marchés ; noms des correspondants à l'étranger, des sous-traitants et revendeurs ; noms et coordonnées du personnel, service par service. Pourquoi ne pas imaginer un concurrent qui envoie de faux courriers par voie électronique par exemple à des clients de *Ventili* en annonçant une incapacité fournir les pièces dans les délais prévus et en annulant même des commandes ?

Autant de cas de figure auxquels pensent souvent Eric Chatran et Pierre Darmond. Mais jusqu'à présent, ils se félicitent de ne pas y être confrontés au sein de *Ventili*.

Le management de connaissances

Appelé aussi knowledge management, le management des connaissances est évidemment précieux pour *Ventili*. L'entreprise s'inscrit dans un environnement caractérisé par des flux importants d'informations qui intègrent des connaissances nouvelles. De là, découle une nécessaire gestion et organisation des connaissances. Elles sont donc classées par grandes thématiques et contribuent à rendre *Ventili* la plus concurrentielle possible ; et cela de manière durable. Car ce qui fait aussi la différence, au-delà de la qualité du produit proposé et de la gamme disponible, c'est la capacité de la société à gérer ses ressources matérielles et immatérielles. Il faut donc avoir identifié le patrimoine informationnel et son rôle en intelligence économique, et se munir des outils et méthodes qui permettent de le protéger.

Car toute la démarche quotidienne de Pierre Darmond et des divers directeurs est guidée par des questions essentielles : quelle est la réalité du marché sur lequel me placé-je ? Quels sont les concurrents auxquels je suis confronté ? Représentent-ils une réelle menace ? Y a-t-il de nouveaux produits ? Dépassent-ils en performance ceux sur lesquels repose notre stratégie commerciale ? Ces produits émergents menacent-ils nos perspectives de développement ?

« Points Clefs Formation »

Acquérir une culture de la précaution

En amont, il faut sensibiliser le personnel accrédité pour s'appliquer à ce type de fonction. La révolution des mentalités est donc essentielle. Et sans doute la plus délicate à faire aboutir. Tout repose là encore sur la dimension des relations humaines, en sensibilisant les intéressés aux enjeux vitaux pour l'entreprise, en fortifiant un esprit de groupe ou de corps – pour reprendre une expression militaire qui définit la cohésion de la troupe d'une même entité – En clair, il s'agit de contribuer au changement de la culture collective du personnel des différents services pour les aider à se redéployer face aux nouvelles cibles du renseignement économique.

C) Maîtriser ses contacts avec l'extérieur

Au sein de *Ventili*, grâce aux nombreuses démarches de sensibilisation effectuées par la direction, les employés savent combien est précieuse la capacité à faire preuve de curiosité. Pas question de cantonner le suivi des nouveautés scientifiques et des grandes manifestations de communication aux seuls chargés de ces mêmes secteurs de *Ventili*. C'est bien l'affaire de chacun des membres du personnel de *Ventili*. Quel que soit leur niveau de responsabilité ou d'implication dans l'entreprise. Mais, en retour, il s'agit aussi d'être vigilant face à toute tentative adverse destinée à déstabiliser *Ventili* ou affaiblir son potentiel productif et commercial.

Organisation d'une journée porte ouverte

Ne serait-ce que lorsque la société réalise une journée « portes ouvertes », des réunions préalables sont organisées. Elles permettent de désigner les locaux accessibles ou non au public, de mettre en place un protocole de surveillance et de sécurité. Il faut en effet éviter tout vol de marchandises, de données techniques et de composants spécifiques. Rien ne doit être laissé au hasard. Même l'accès aux toilettes doit être scrupuleusement balisé pour éviter de surprendre un visiteur, qui se dira alors perdu ou égaré, à proximité du bureau d'études.

Il ne faut pas douter du fait qu'une opération « Portes ouvertes » est, par définition, une bonne opportunité pour les concurrents désireux de découvrir de l'intérieur la société. Ils peuvent aussi repérer des employés qui, sondés par discussion apparemment innocentes, peuvent paraître relativement malléables et influençables.

Néanmoins, la direction de *Ventili* peut se réjouir. Aucune effraction ou situation anormale n'a été observée à l'occasion de ces journées particulières.

Mais cela n'a pas toujours été le cas lors de visites d'une délégation étrangère.

Visite d'un client potentiel

La prudence a pourtant toujours été de mise lorsque la société reçoit une délégation étrangère, et plus particulièrement quand il s'agit d'une délégation asiatique. Or, il est arrivé que certains membres d'une délégation chinoise, derrière l'image rassurante de personnes humbles envers leurs hôtes, admiratives devant les infrastructures visitées, aient feint la curiosité pour s'approcher de postes de travail, récupérer des éléments de matière première métallique avec de semelles aimantées et tremper le bout de leur cravate dans un bac de peinture. Un ingénieur de *Ventili*, délégué au responsable qui assurait la visite au profit de la délégation, se rendit compte de ce qui se passait. Eric Chatran et Pierre Darmond furent très rapidement mis au courant et les suspects poursuivis en justice pour espionnage industriel.

« Points Clefs Formation »

Vigilance lors de la visite de délégations

Dans un premier temps, vous devez disposer des identités de chacun des membres de la délégation attendue. Lors de sa visite, il faut soigneusement encadrer ladite délégation avec des cadres rompus à ce type d'exercice, sans laisser paraître vigilance et rigueur. En tout cas, il ne faut rien laisser au hasard.

Une autre menace pèse sur *Ventili* : celle de la contrefaçon.

Appréhension de la contrefaçon

« Il faut en effet être prudent dans la démarche d'extension de notre influence commerciale » tempère régulièrement Pierre Darmond. Le directeur *Ventili* hésite à lancer sur le marché chinois une nouvelle gamme de ventilateurs qui, en Europe orientale et méditerranéenne, remporte pourtant un franc

succès. L'entreprise française avait ainsi réussi à mettre au point un ventilateur conciliant qualité des matières, robusticité et fort rendement sans consommation énergétique excessive. Fruit réel d'un succès commercial, le ventilateur doit-il pour autant être exporté jusqu'en Chine ? Interrogation qui obsède les Services Marketing et de Communication de *Ventili*. La direction, de son côté, craint les répercussions néfastes pour l'entreprise sachant que le territoire chinois rassemble un secteur considérable de la contrefaçon. Un secteur qui bénéficie pleinement des principes de l'espionnage industriel. Il favorise la conception de produits comparables à leur modèle occidental, mais en moins bonne qualité, et diffusé sur le marché français. En retour, l'entreprise française, qui privilégiait la finition et la durabilité de son produit, ne risque-t-elle pas de péricliter ? C'est pourquoi Pierre Darmond ne veut pas s'exposer dangereusement en cherchant à pénétrer le marché asiatique.

« Points Clefs Formation »

La menace de la contrefaçon

Les statistiques de la Communauté Européenne pour 2006 montrent que le nombre de saisies de marchandises portant atteinte à des droits de propriété intellectuelle, de même que le nombre d'articles saisis, a augmenté de manière spectaculaire par rapport à l'année antérieure. Les fonctionnaires des douanes ont intercepté en 2006 plus de 128 millions d'articles contrefaits ou pirates, au cours de 37 334 opérations de saisie.

En comparaison de l'année antérieure, où les douanes avaient saisi 75 millions d'articles à l'issue de 26 000 opérations, ces chiffres traduisent une augmentation énorme du nombre d'articles saisis ainsi qu'une forte intensification des activités des douanes dans ce domaine.

Participer à un colloque ou un salon en France ou à l'étranger

Comme nous l'avons vu à maintes reprises, les membres de l'entreprise *Ventili* sont attentifs à ce qui se dit, s'écrit et se prépare dans l'environnement immédiat ou périphérique ; tant dans le domaine scientifique qu'en matière de communication. En soit, les colloques ou les salons sont des évènements-clés qui constituent d'appréciables atouts : pour se faire connaître comme pour obtenir des informations.

« Points Clefs Formation »

S'imprégner de l'environnement professionnel

En cela, il faut qu'à votre niveau, et en fonction du degré d'implication dans la vie de notre entreprise, vous vous fassiez le relais d'informations sur les manifestations qui se tiennent non seulement sur le territoire régional, mais également dans les plus lointaines sphères géographiques, y compris à l'étranger.

Lors de la tenue d'une conférence ou d'un colloque qui peut intéresser directement votre secteur d'activité, il faut y dépêcher un collaborateur capable de vous en rapporter la quintessence. Cela s'intègre donc dans les techniques d'acquisition des informations de terrain, qu'elles soient de sources humaines ou informelles.

En corrélation avec cette démarche méthodique à plusieurs entrées, il faut garder à l'esprit la nécessité d'être en conformité avec les règles et principes établis par le droit, l'éthique et la déontologie de l'acquisition puis de l'utilisation de l'information.

Les conférences font également partie des sources d'informations et présentent une valeur ajoutée très importante dans la conduite d'une démarche de veille stratégique.

Quelle que soit la nature de la manifestation visée – salon, colloque ou conférence – le fait de s'y rendre nécessite un minimum de précautions dans les déplacements et, s'il s'impose, les conditions de l'hébergement.

Georges Messonot, cadre commercial de *Ventili*, n'est pas prêt d'oublier son voyage au Salon national de la ventilation. A bord du train, il avait fait preuve de la plus grande vigilance pour ne pas risquer la perte ou le vol tant de son ordinateur portable que des documents de travail en sa possession. Il avait pris garde à ses voisins, de peur que quelqu'un prenne connaissance des documents papiers, ou informatisés, en utilisant un matériel électronique adapté. Il avait gagné son hôtel, à la fois soulagé et tout heureux d'avoir échappé à tout problème. Pour lui, c'était une petite victoire. Il se faisait tard. Il avait faim. Il déposa rapidement ses affaires dans sa chambre puis se rendit dans un restaurant du centre-ville ; une bonne adresse que lui avait conseillé un proche.

Autre moment critique pour vos documents, sur papier ou informatique, votre passage à l'hôtel. Or, durant son absence, considérez que sa chambre

fut visitée et ses documents copiés. Un mystérieux visiteur, diligenté par un puissant concurrent venait d'obtenir de précieuses informations professionnelles.

« Points Clefs Formation »

Des rencontres à double tranchant

Il arrive même que des rencontres apparemment fortuites conduisent votre interlocuteur à vous « harponner ». Au fil du temps – car cela s'inscrit sur le long terme – il peut vous rendre tributaire de sa dite amitié, de ses efforts pour vous venir en aide même sur le plan personnel. Méfiance donc à l'égard des rencontres trop rapidement chaleureuses.

Une fois sur le lieu du Salon, il faudra redoubler de vigilance et de prudence. Gardez soigneusement vos affaires, n'exposez et ne dévoilez rien de capital pour l'entreprise que vous représentez. Et si au cours de votre visite du Salon, il vous arrive d'entamer une discussion avec des représentants d'autres concurrents, prenez du recul par rapport à ce qui peut vous être dit ; en matière de ventes, de capacités de production de ladite entreprise, de diffusion à l'international, de nombre de sites de production, d'employés. Si vous observez que votre interlocuteur a tendance à largement dévoiler les activités de son entreprise, cela peut parfois être tentant, plus ou moins consciemment, de parler des activités de votre entreprise. Et, de la sorte, sans prendre garde, vous transmettez des éléments précieux, des données actuelles, alors que ce que vous aurez entendu peut être, à l'inverse, dépassé, grossi ou tout simplement faux…

L'analyse risque-pays

Lorsque la santé de votre entreprise est solide, que votre chiffre d'affaire est assez consistant ou, à l'inverse, que vous connaissez des risques d'asphyxie qui vous incitent à élargir votre marché de distribution, vous vous penchez sur de nouvelles zones géographiques où vous pourriez étendre vos activités. Mais, avant tout, il vous faut réunir des informations précises sur l'environnement socio-économique et surtout politique des pays considérés : y a t-il ou non risque de déstabilisation en raison de tensions intercommunautaires ; y a-t-il risque de guerre civile ; ou encore, est-ce que les Occidentaux sont acceptés ou font-ils l'objet d'une politique de rejet ? En cela, il faut donc rassembler des informations relevant du secteur « Risque-pays ».

« Points Clefs Formation »

Gestion de l'information

L'exploitation de l'information exige l'application de plusieurs étapes :

- Collecte de l'information brute ;
- Validation, analyse et synthèse de cette information ;
- Interprétation et diffusion de l'information, source de connaissance ;
- Appui et soutien de l'échelon décisionnel qui est donc inspiré par ladite information/connaissance.

Les analyses risques-pays peuvent être assurées par des spécialistes, géopoliticiens indépendants ou par des cabinets œuvrant dans ce domaine. De même, il n'est pas inopportun de solliciter le pôle « Risque-pays » du ministère des Affaires étrangères. Si vous en avez la possibilité tant matérielle qu'humaine, vous pouvez créer votre propre équipe de spécialistes pour traiter ces questions. Vous pouvez aussi effectuer quelques voyages à l'étranger, dans les zones visées, éventuellement accompagnés par les organismes publics spécialisés (point d'appui à l'international, par exemple). Si vous constatez que votre projet d'extension commerciale se destine à une zone instable, en proie à la guerre civile ou à de tensions sociales très fortes, vous jugerez alors préférable d'annuler le projet ou de le porter sur une zone géographique plus stable. Inutile en effet d'exposer votre personnel expatrié à un enlèvement contre rançon ou de risquer les détournements de marchandises, sauf à vous faire, là aussi, accompagner par des spécialistes.

« Points Clefs Formation »

Un rapport de l'Institut des Hautes Etudes de la Défense nationale (IHEDN) paru en 2000 précise que près de 90% des entreprises interrogées reconnaissent évoluer dans un contexte de guerre économique. Curieusement, ce pourcentage tombe à 50 % lorsque les entreprises doivent exprimer une situation de menaces concurrentielles.

« Points Clefs Formation »

- Préserver coûte que coûte l'information et disposer des meilleurs atouts pour la collecter et l'exploiter au profit de l'entreprise.
- L'information doit faire l'objet d'une gestion appropriée, entre précaution, discrétion et rigueur.
- L'information doit être sectorielle et donc répartie entre les divers pôles de l'entreprise à partir du Service de veille informatique.
- Les circuits de transmission et de distribution de l'information doivent être sécurisés à l'extrême afin d'éviter toute fuite ou captation hostile.
- De même, les employés et partenaires de l'entreprise doivent utiliser les informations en leur possession avec une précaution de tous les instants pour éviter le vol et la divulgation de données qui pourraient mettre en difficulté – ou en péril – les activités de l'entreprise.
- Gardez à l'esprit que certains concurrents sont prêts à tout pour obtenir des informations de tout premier ordre – stratégiques – concernant votre entreprise. Ils peuvent même aller jusqu'aux démarches de débauchages et d'intimidation/chantage.

L'essentiel de l'intelligence économique

En quelques pages, résumons la nature même de l'intelligence économique, à travers ses principes, ses finalités et ses méthodes.

Un état d'esprit adapté...

Tout d'abord, l'intelligence économique repose sur une mentalité particulière. Il faut faire preuve d'une perception lucide, réaliste du milieu de l'économie.

Il faut en effet bien comprendre que les activités économiques s'intègrent sur un ou plusieurs marchés où les rapports de force sont quasiment permanents, avec le risque d'être exposé à des opérations de déstabilisation concurrentielle.

De là, il faut avoir conscience de l'existence de menaces directes contre l'organisation de votre propre entreprise, par divers canaux : humains, technologiques ou commerciaux. Avec la conviction qu'il faut les prévenir. D'où l'importance d'être capable d'anticiper.

... conforté par des moyens d'action légaux

Votre méthode de protection, qui est à la fois stratégique et tactique, doit impérativement reposer sur des moyens légaux, au risque dans le cas contraire de vous faire rentrer dans le domaine éthiquement et pénalement répréhensible de l'espionnage économique.

Le rôle capital de l'information

De toute évidence, votre capacité d'adaptation et de réaction, face à toute forme de menace, repose essentiellement sur l'information, le pôle humain et relationnel, porté par l'atout technologique. En somme, on retrouve les mêmes vecteurs utilisés par vos concurrents et compétiteurs.

L'information permet à la fois de renforcer l'organisation et le potentiel d'action de votre entreprise. Elles contribuent à ce que vos connaissances soient optimales dans votre domaine d'activité, en fonction des données présentes sur le marché.

D'autre part, dans le but de protéger le patrimoine de l'entreprise, l'information doit vous permettre également d'anticiper les éventuelles menaces auxquelles vous pouvez être exposé – espionnage, opérations de déstabilisation, vandalisme, vol, actions terroristes (notamment si vous travaillez dans des secteurs stratégiques).

... au profit de la coordination des acteurs de l'entreprise

Rappelons, si besoin est, que l'intelligence économique exige un travail d'équipe. Elle contribue à la mise au point de la stratégie et des tactiques destinées à renforcer la place de l'entreprise sur le marché, dans un environnement fortement concurrentiel. Ce qui repose donc sur des méthodologies soigneusement établies, en vertu des moyens humains, des moyens d'analyse et de la connaissance dont dispose l'entreprise. L'informatique est alors un vecteur indispensable qui sert, à ce niveau, la coordination et la concertation des divers acteurs de l'entreprise.

Le principe de veille

Il est à la disposition de l'intelligence économique pour la quête permanente d'informations, de données. Il s'applique en fait à plusieurs niveaux au sein de l'entreprise, de manière complémentaire.

Si bien que l'on remarque notamment la veille informatique, la veille concurrentielle, ou même les veilles technologiques et sociales (liées directement à la gestion des ressources humaines). Il est assuré par un personnel qualifié et de confiance, parfaitement rôdé au principe de l'intelligence économique, en contact étroit avec la direction de l'entreprise.

L'intelligence économique en France

La France, comparée aux pays anglo-saxons notamment, a tardivement adopté les principes même de l'intelligence économique. Le point de départ est marqué par la publication en 1994 du rapport du Commissariat Général du Plan, intelligence économique et stratégies des entreprises ; rapport dirigé par Henri Martre, ancien PDG de l'Aerospatiale. En 1997, est créée l'Ecole de guerre économique, à l'initiative de Christian Harbulot (son directeur), et du Général Pichot-Duclos. Tout concourt à la prise en compte des affrontements autour d'informations au niveau de la stratégie des entreprises, sur fond de mondialisation des échanges de plus en plus conflictuelle.

En décembre 2003, Alain Juillet est nommé Haut Responsable chargé de l'intelligence économique au sein du Secrétariat Général de la Défense Nationale (SGDN). Résultat d'un choix politique inspiré du rapport du député Bernard Barrayon remis en juin 2003, au Premier Ministre et intitulé *intelligence économique, compétitivité et cohésion sociale.*

Depuis 2005, les actions gouvernementales s'accélèrent avec la mise en place notamment des pôles d'intelligence économique au sein des principaux Ministères (Affaires étrangères, Intérieur, Défense, Economie, Finances et Industries), et la création d'une fédération des professionnels de l'intelligence économique.

La loi du 13 août 2004 ayant reconnu le rôle de « Chef d'orchestre » du développement économique aux régions, celles-ci interviennent au travers des schémas régionaux de développement économiques (SRDE), en appui de l'appropriation par les PME de l'intelligence économique.

En résumé

Ainsi, l'intelligence économique repose-t-elle essentiellement sur des méthodes offensives et défensives, qui permettent la coordination des actions de recherche, de traitement et de transmission de l'information à haute valeur ajoutée. Celle-ci est avant tout sélectionnée, triée puis distribuée, pour être ensuite exploitée – ou utilisée – par les principaux acteurs de l'entreprise. Ceux-ci sont organisés en réseau – interne et externe (fournisseurs, clients, partenaires, contacts) à l'entreprise – organisés autour de la direction, responsable du management de l'entreprise qui s'assure de la préservation de données stratégiques de l'entreprise (appelées aussi mémoire en référence à des informations obtenues par le biais de l'intelligence économique).

L'importance de l'intelligence économique est devenue telle qu'elle est désormais inscrite à l'échelle des relations interétatiques. Les Etats souhaitent ainsi protéger les entreprises qui œuvrent dans des secteurs sensibles, notamment liés à la Défense nationale. Cela se traduit par la mise en place de mesures de contrôle des investissements étrangers dans les grandes entreprises, notamment dans le transport maritime, dans le secteur de la pétrochimie et des hydrocarbures, de certains médias. Et sont désormais considérées comme particulièrement sensibles, les secteurs de l'armement, de la cryptologie, des biotechnologies, etc.

Conclusion

Loin de vouloir favoriser une approche alarmiste et propice à un tout sécuritaire, l'entreprise *Ventili* a tout de même intérêt à faire face collectivement aux véritables défis économiques qui se présentent à elle dans le cadre de l'internalisation – toujours grandissante – des échanges.

La mondialisation des circuits économiques contribue à conforter les démarches de concurrence aigue. Il faut donc insister sur les besoins de surveillance, notamment technologique. Parallèlement, il faut éviter les excès de suspicion. Il ne faut pas se laisser envahir par un sentiment de menace exacerbé qui incite l'entrepreneur à procéder à la surveillance même de ses employés, en dehors parfois de l'environnement professionnel.

Autre élément de méthode à garder à l'esprit, le recoupement de l'information est indispensable. Et à plus d'un titre en sollicitant plusieurs sources. On peut ainsi valider, de manière transversale, des données qui, erronées, peuvent conduire à de mauvais choix stratégiques. Voire même à de graves préjudices humains : licenciements abusifs, mauvaise perception de tel ou tel employé selon une rumeur, idées préconçues et infondées, mauvais choix commerciaux selon des rumeurs ou une « intoxication », etc.

En fait, l'intelligence économique ne peut être efficace qu'en reposant sur une culture de partage au sein de l'entreprise. Elle s'exprime à travers des choix clairement établis, en fonction de ses propres aspirations, de ses priorités et de la prise en compte de la réalité des menaces. L'intelligence économique constitue donc bien une doctrine d'action, d'anticipation et de prévention qui combine les éléments issus du monde de l'information, du renseignement, de la stratégie et bien entendu de l'économie.

Et par extension, l'entreprise doit s'imprégner d'une nouvelle réalité qui a toute son importance dans la conjoncture actuelle. Elle doit être convaincue qu'en appartenant au secteur privé, elle est néanmoins responsable d'une nouvelle territorialité, membre d'une nouvelle stratégie au profit de l'économie nationale, du patriotisme économique.

L'intelligence économique s'intègre donc dans la géoéconomie, sachant que les espaces sont en interrelations économiques, soit selon les principes du partenariat, soit sur les bases de la concurrence. Depuis trente ans, le capitalisme connaît de profondes mutations avec un durcissement continu de la concurrence et un nombre grandissant d'acteurs économiques. Ceux-ci s'affrontent pour la conquête de marchés dont le nombre, à l'inverse, n'est pas extensible ni proportionnel. Les enjeux de pouvoir, avec la fin de la guerre froide et d'un monde bipolaire, se sont donc déplacés sur le camp économique. Au point de faire apparaître les puissants comme étant ceux qui disposent des ressources financières les plus importantes et des meilleures stratégies de gestion, atouts du pouvoir réel. L'Etat, à son niveau, doit être convaincu de s'appuyer sur un tissu d'entreprises nationales, selon les critères de nationalité économique : structuration financière, stratégies de recherche-développement, territorialité, environnement institutionnel, origine culturelle du management.

Enfin, dernier point essentiel : il faut mettre en avant les notions d'intéressement des employés à la vie de leur entreprise. Car l'être humain est naturellement le pôle central des activités économiques. Il doit le rester, avec le souci de l'excellence et de la pugnacité professionnelle.

Lexique

Analyse de sécurité informatique (computer security analysis) : Méthode consistant à faire le point sur tous les risques informatiques (risques gradués) et les parades possibles au sein d'une structure particulière, en tenant compte des impératifs organisationnels et des contraintes administratives et financières, humaines et logistiques. L'analyse peut aussi être effectuée au moment de la planification d'un projet.

Analyse/Traitement : les informations réunies sont ensuite analysées, répertoriées et traitées. Certaines, jugées finalement sans portée, peuvent être éliminées.

Anti-virus : Programme informatique qui permet de détecter, identifier et éliminer les virus de diverses catégories présents dans votre système.

Audit de sécurité » informatique : Démarche qui conduit à l'examen et à l'évaluation des moyens réels ou nécessaires pour assurer la sécurité informatique au sein d'une organisation. Le but étant d'assurer l'intégrité et la sécurité des données.

Authentification : Procédure de vérification afin de s'assurer, si nécessaire, du niveau de confiance entre l'identifiant et la personne utilisatrice lors de l'accès à un réseau, à un système informatique ou un logiciel.

Attaque informationnelle : Méthode offensive visant à obtenir, conformément à un plan prédéfini, des informations de première importance.

Bluetooth : Système d'ondes radio, lancée en 1998, qui permet le lien sans fils d'un assistant personnel, d'un téléphone ou d'un ordinateur portable, à une oreillette ou à un ordinateur fixe.

Cadenas (Padlock) : Icône destinée à informer qu'une page web, en cours de consultation, est issue ou non d'un serveur qui a recours au chiffrement des données.

Cheval de Troie (Trojan Horse) : Nom donné à un programme type-virus qui, sous l'apparence d'un programme standard, réussit à contourner le système de sécurité informatique et à pénétrer les fichiers désirés. Il peut alors les consulter ou les détruire.

Chiffrement : Confidentialité des données assurée par un mécanisme de sécurité.

Clé : Composante d'une procédure de sécurisation et de secret qui permet de coder ou chiffrer, puis de déchiffrer un message, à partir notamment d'algorithmiques symétriques et asymétriques.

Collecte : Démarche consistant à réunir des informations thématiques, non seulement par internet mais aussi par d'autres canaux (rencontres, dialogues, tables rondes, etc..).

Contrôle d'accès : Application d'une authentification de personne – autorisée – pour accéder à un lieu particulier ou à un système informatique précis.

Cookie (témoin) : Ce fichier est chargé sur l'ordinateur d'un internaute à partir de certains sites visités. Il vise à reconnaître l'ordinateur utilisé lors de la consultation.

Cracker (pirate) : Nom donné à un spécialiste en informatique qui, en toute illégalité, pénètre des systèmes d'exploitation, en violant les systèmes de sécurité et/ou copie des logiciels.

Cryptage : Opération visant au « chiffrement » d'un message qui devient alors codé. Il ne peut être exploité que par son destinataire qui dispose des clés de décryptage ou « déchiffrement ». Ce système est couramment employé pour les opérations bancaires sur le net.

Cryptanalyse : Ensemble des mesures de décryptage sans connaissance préalable des clés de chiffrement. Cela permet d'évaluer la sécurité des programmes de chiffrement requis en cryptographie.

Cryptogramme : Message devenu incompréhensible grâce à une procédure de chiffrement. Seuls les détenteurs d'une clé et d'un algorithme peuvent le déchiffrer.

Désinformation : Procédé par lequel on induit en erreur des personnes en falsifiant l'information. Ce qui est aussi considéré comme une opération d'intoxication.

Déstabilisation : Action reposant sur une combinaison de facteurs et de moyens destinée à perturber sérieusement une personne, une entreprise ou une institution et les activités qui y sont liées.

Données stratégiques : Informations d'importance capitale pour le bon fonctionnement d'une institution, d'une entreprise.

Entente de sécurité : Mise au point des règles de sécurité établies dans les interactions avec la clientèle ou entre deux interlocuteurs institutionnels.

Espionnage : Action qui consiste à connaître les modalités ou caractéristiques de fonctionnement d'une institution, de même que sur sa politique commerciale, par exemple. Elle peut aussi se concentrer sur le facteur humain, afin d'obtenir des informations précises à l'insu de la personne visée.

Etreinte mortelle : Expression utilisée pour définir le blocage d'un système informatique, suite à une attaque par virus, ou par l'interaction de deux programmes qui travaillent simultanément sur deux types de fichiers qui auto bloquent les deux programmes.

Faille de sécurité : Le système informatique est déclaré faillible. Le défaut du programme est découvert par des pirates informatiques (hackers ou script kiddies) qui peuvent alors pénétrer le réseau informatique.

Géopolitique : Etude des rapports entre les politiques des Etats et les espaces géographiques, et par extension des politiques engagées en fonction des besoins économiques et militaires desdits Etats.

Géoéconomie : Implication des politiques économiques sur les espaces géographiques, naturels et humains.

Gestion des risques (risk management) : Procédure préalable destinée à mesurer les risques auxquels s'expose une démarche commerciale, une politique particulière. En conséquence de quoi sont établies les mesures préventives (procédures de contrôles, opérations de couverture) adaptées aux risques définis (insolvabilité de clients, risques d'accident d'exploitation, retards des fournisseurs, inflation, destruction de biens, violation d'un système informatisé).

Gestion des risques informatiques : Adoption de mesures destinées à contrer le plus efficacement possible les risques informatiques prédéfinis.

Habilitation de sécurité : Droit par lequel un utilisateur peut avoir accès à des données ou à des fichiers précis, considérés comme sensibles ou d'importance stratégique.

Infiltration : Méthode qui consiste à pénétrer une structure particulière, de manière clandestine ou occulte.

Interface sécuritaire : Ensemble des normes et mécanismes de sécurité pour permettre le contact et l'échange avec une clientèle ou un interlocuteur particulier.

Internet : Réseau informatique interconnectant de couverture mondiale.

Intrusion : Démarche de violation d'un système ou d'un réseau dans le but de saisir des informations généralement confidentielles ou dans le but de compromettre le bon fonctionnement du réseau.

IP (Internet Protocol) : Protocole d'échange d'informations généralisé sur le réseau Internet et les réseaux d'entreprise.

IPsec (IP Security Protocol) : Sécurisation des échanges sur réseau IP par la mise en place d'une authentification mutuelle et le chiffrement des données.

Key Loger : Programme espion qui permet d'enregistrer toutes les opérations informatiques effectuées sur un ordinateur donné : frappe, sauvegardes réalisées, consultation de sites particuliers sur internet.

LAN : Réseau local dit interconnectant qui relie les équipements informatiques d'une structure privée et géographiquement réduite.

Log : Fichier géré par un serveur et chargé de mémoriser les paramètres de chaque connexion.

Mail Bombing : Démarche de malveillance qui consiste à envoyer un nombre considérable de messages à une adresse de courrier électronique.

Mécanisme de sécurité : Système mis en place, à partir de moyens électroniques ou matériels, pour établir une sécurité informatique.

Moteur de recherche : Logiciel qui permet, à partir de mots-clés et de liens hypertextes, de trouver tous les fichiers, les images et vidéos qui y sont associés.

Patriotisme économique : Combinaison de capacités économiques et politiques pour attirer l'activité productive à haute valeur ajoutée et mettre en valeur les capacités d'un pays dans un contexte de concurrence mondialisée. Il repose sur les compétences, les savoir-faire et les motivations culturelles et géoéconomiques.

PDA : Assistant personnel numérique pour Personal Digital Assistant. Cet outil électronique combine, entre autres programmes, agenda et répertoire.

Pare-feu (firewall) : Programme de protection d'un réseau interne face à toute intrusion extérieure. De même, il interdit tout échange non autorisé entre l'intérieur et l'extérieur.

Phishing : Technique frauduleuse utilisée pour récupérer des informations, le plus souvent bancaires, sur le net, au détriment d'internautes. Elle repose sur l'usurpation d'identité (d'entreprise ou d'institution bancaire par exemple).

Phreaker (pirate du téléphone) : Personne qui pénètre les réseaux de télécommunications via internet afin de pouvoir, frauduleusement, téléphoner en toute gratuité.

Pirate (Hacker/Cracker) : Terme qui désigne toute personne qui viole l'intégrité d'un réseau informatique, soit pour voler des programmes ou des fichiers, soit pour dupliquer des données.

Pression psychologique : Action de déstabilisation destinée à soumettre à un sentiment d'insécurité la personne visée. A terme, cela peut conduire à un chantage reposant sur des critères de menaces.

Proxy : Service qui fragmente une communication établie entre un serveur et un client. Un premier contact est activé entre le client et le firewall, suivi d'un deuxième entre ce même firewall et le serveur.

Rétro-virus : Virus destiné à contrer l'action d'un ou plusieurs logiciels antivirus.

Screenshot (capture d'écran) : Enregistrement de ce qui apparaît à l'écran (graphique, texte) dans un fichier donné.

Sécurité informatique : Méthode appliquée à partir d'un ensemble de mesures technologiques, administratives ou physiques afin de protéger des biens informatiques et les informations qu'ils contiennent selon le principe de la confidentialité. Elle permet d'assurer le bon fonctionnement du parc informatique d'un service ou d'une entité plus ou moins étendue. Elle intègre donc les notions d'habilitation / accréditation, mots de passe, le chiffrement pour la consultation, sans oublier la protection et la surveillance des locaux concernés.

Sniffer : Programme qui permet de saisir des données en circulation sur un réseau informatique. Il vise aussi à détecter des mots de passe ou des éléments destinés à violer les systèmes de sécurité.

Spam : Message envoyé à un groupe de personnes considéré comme nuisible par les programmes antivirus.

SSL (Secure Socket Layer) : Procédure de sécurisation des échanges sur internet qui repose sur l'authentification, l'intégrité et la confidentialité.

Stratégie : Politique particulière mise en place à partir de diverses étapes et tactiques coordonnées, afin d'atteindre un objectif précis.

Système d'information (SI) : Ensemble programmé pour traiter l'information.

Tactique : Composante de la stratégie et qui, combinée à d'autres facteurs, contribue à atteindre le but recherché.

Tiers de certification : Structure de gestion et d'attribution de clés publiques à des personnes identifiées et reconnues.

Tiers de confiance, de certification ou de séquestre : Structure de gestion et d'attribution de clés de chiffrement ou d'authentification.

Veille informatique : Méthode consistant à réunir des informations et renseignements à partir de mots clés ou de serveurs précis. Cela donne lieu, dans un second temps, à une gestion et exploitation des informations triées et sélectionnées en fonction du degré d'importance et de pertinence.

Virus : Programme qui est chargé de se répandre dans un réseau à travers les divers ordinateurs et qui peut s'auto-répliquer, en procédant à des opérations de nuisance plus ou moins graves ; du ralentissement de l'unité à la destruction de données.

Wi-fi (ou WIFI – Wireless Fidelity) : Réseau informatique sans fil destiné initialement à un fonctionnement en réseau interne. Aujourd'hui le WIFI permet une liaison à haut débit à internet. Ce réseau correspond à la norme internationale 802.11 de l'Institute of Electrical and Electronics Engineers. La certification est définie par Weca (Wireless Ethernet Compatibility Association).

WLAN (Wireless LA) : Réseaux locaux sans fils.

Zone sensible : Secteur stratégique d'une entreprise, primordial à son bon fonctionnement. Il conserve des informations et moyens matériels qui doivent être impérativement protégés et soumis à des entrées sur accréditation.

ANNEXES

La actions du Conseil Régional d'Ile-de-France

Dans le cadre du Schéma régional de développement économique, adopté en 2006, le Conseil régional a engagé de nombreuses initiatives pour encourager et appuyer la mise en œuvre de l'intelligence économique et stratégique (IES) par les PME-PMI d'Ile-de-France.

En premier lieu, l'ensemble des aides individuelles aux entreprises permet aujourd'hui d'intégrer des prestations d'IES.
Ainsi le dispositif Cap Entreprise, qui peut prendre en charge jusqu'à 6 jours de formation et 3 jours de conseil au profit des jeunes dirigeants d'entreprise, ou le bouquet d'aides régionales, qui propose à des PME en forte croissance de bénéficier d'une subvention de 200.000 à 250.000 € pour être accompagnées dans leur projet de développement par des consultants experts (conseil stratégique, accompagnement à l'export, investissement, aide au recrutement).

Les entreprises sont également encouragées à se regrouper pour s'organiser en réseaux, monter des projets collectifs, déceler des marges de productivité, mutualiser les coûts de leur développement – notamment à l'international. Ces projets ont souvent pour moteur ou condition de succès une démarche d'IES.
Un certain nombre d'aides existe, qui permettent de bénéficier de prestations d'information et de formation, de diagnostic, d'accompagnement individuel et collectif. Les entreprises peuvent également accéder à des services mutualisés, comme des plateformes de veille collaborative, dans le cadre des programmes de développement des filières prioritaires.
Par ailleurs, les pôles de compétitivité, soutenus par les pouvoirs publics et les acteurs académiques et industriels des filières d'excellence franciliennes, ont en charge la mise en œuvre d'outils de veille et/ou des actions d'intelligence économique à l'usage de leurs membres.

Enfin, une cellule régionale d'intelligence économique territoriale doit être organisée en 2008 afin de déceler en amont les menaces et les opportunités nécessitant une réponse rapide et coordonnée des pouvoirs publics afin de conforter les entreprises et les emplois de la région.

Renseignements :
Direction du développement économique et de l'emploi
Mission intelligence économique et stratégique
Tél. : 01 53 85 57 23 / fax : 01 53 85 60 49

Région de Gendarmerie Ile-de-France

La Gendarmerie, un acteur de la sécurité économique
Protéger et Conseiller

Depuis 2005 le dispositif « intelligence économique »de la gendarmerie se décline de la direction générale jusque dans chaque département. La chaine ainsi constituée, composée de personnels spécialisés, s'appuie sur un réseau d'environ 4000 unités, réparties sur 95 % du territoire national. En Ile-de-France, 120 brigades territoriales sont autant de points d'entrée destinés à satisfaire les besoins de sécurité du public. Ce maillage du territoire dans l'espace est un atout, notamment dans le domaine de la surveillance et du renseignement.

Compétente pour toutes les affaires de police judiciaire qui intéressent la sécurité économique (vols de fret, d'ordinateur, racket,etc.) la gendarmerie a par ailleurs développé des expertises particulières pour faire face aux nouvelles formes de la criminalité. Elle dispose ainsi d'enquêteurs N-Tech (nouvelles technologies) pour lutter contre la cybercriminalité et de spécialistes en matière d'analyse financière criminelle. A cet égard les PMI/PME ne doivent pas hésiter à signaler à leur brigade de gendarmerie de rattachement tout fait suspect.

La gendarmerie contribue, aux côtés des autres services de l'Etat, à la protection du patrimoine physique et intellectuel, à la détection des risques, menaces ou vulnérabilités qui pèsent à l'échelon local. Elle participe pleinement à la sensibilisation des agents économiques, notamment des PME/PMI souvent sous-traitants de grandes entreprises.

En outre, la gendarmerie s'investit dans la dynamique de promotion de l'intelligence économique à travers l'action de l'institut d'études et de recherche sur la sécurité des entreprises (IERSE). Cet organisme participe, en effet, à la sensibilisation et à la formation de chefs d'entreprises, de cadre de l'administration, d'élus et des référents régionaux de la gendarmerie."

CGPME Ile-de-France

La voix des PME en Ile-de-France

La CGPME Ile-de-France est la seule organisation spécifique aux dirigeants de PME franciliens. La mobilisation constante de la CGPME permet d'obtenir de véritables avancées pour gagner en souplesse, avec le recours facilité aux heures supplémentaires, avec la révision des seuils d'effectif et la réduction des délais de paiement. Pour diminuer les charges : notre engagement a porté ses fruits, avec la suppression de l'Imposition Forfaitaire Annuelle dès 2009.

S'appuyant sur un réseau dense d'entreprises et de Branches adhérentes, la CGPME Ile-de-France est l'interlocuteur des acteurs politiques et institutionnels : branches professionnelles régionales, syndicats de salariés, organisations consulaires, universités…

Faciliter la vie des PME

Attentifs aux préoccupations et aux besoins quotidiens des PME, la CGPME Ile-de-France les assiste et les conseille. Cette démarche collective permet de briser l'isolement de dirigeants, en leur permettant de confronter leurs expériences et leurs difficultés. Ensemble, ils participent à des projets, dans les domaines économiques, social, fiscal, de la formation et de l'international. Les solutions apportées par la CGPME Ile-de-France leur permettent de gagner du temps pour pouvoir se consacrer pleinement au développement de leur entreprise.

Un réseau qui défend les PME

La CGPME Ile-de-France et toutes les CGPME départementales sont présentes dans les institutions qui comptent pour les PME : Conseil des Prud'hommes, Commission départementale des impôts, Chambre de Commerce et d'Industrie de Paris, Tribunal de Commerce de Paris, Tribunal des Affaires Sociales, ASSEDIC, CPAM-CAF, Universités, COTOREP… Là où des hommes et des femmes s'engagent bénévolement pour la défense des PME et la prise en compte de leurs intérêts.

En adhérant dans une fédération départementale, une PME :

- bénéficie de services spécifiques : information, protection, formation..
- s'intègre à un puissant réseau,
- dialogue avec les responsables des fédérations afin de pouvoir résoudre rapidement ses difficultés,
- renforce les messages à destination des pouvoirs publics pour défendre les PME françaises.

La gestion paritaire de la formation professionnelle

Une partie de la contribution due par les entreprises pour le développement de la formation professionnelle continue est administrée par les partenaires sociaux au sein d'organismes paritaires créés par voie d'accord collectifs et agréés par l'Etat : les organismes paritaires collecteurs agréés (OPCA), en particulier le premier OPCA interprofessionnel en Ile-de-France en termes de volume financier, qui est AGEFOS PME Ile-de-France. Ils gèrent les dispositifs qui relèvent du pouvoir de décision du chef d'entreprise, en accompagnant les entreprises et en finançant leurs outils : plan de formation

des salariés, Droit Individuel à la Formation, parcours de formation plus longs avec notamment les périodes de professionnalisation pour les salariés ou démarche de recrutement et de formation en alternance avec les contrats de professionnalisation.
Pour ce qui relève des congés formation à l'initiative du salarié (congé de bilan de compétences, congé individuel de formation), la gestion est régionale et interprofessionnelle (FONGECIF).
Le développement de l'enseignement professionnel et l'apprentissage avec l'AGEFA PME de telle sorte que les jeunes accèdent tant au développement professionnel que social. Ces actions nécessitent des ressources, c'est pourquoi AGEFA PME est collecteur de la taxe d'apprentissage selon le régime de la convention générale de coopération signée avec le ministère de l'éducation nationale et de la recherche le 1er août 2005. AGEFA PME développe ainsi des actions qui concernent l'orientation, l'européanisation des formations professionnelles, la coopération technologique, la création de dispositifs éducatifs multimédias. Pour asseoir sa démarche, les instances d'AGEFA PME ont créé un observatoire qui a pour mission de mettre en perspective les pratiques actuelles de l'apprentissage et de l'enseignement professionnel au regard des actions qu'elles souhaitent mettre en œuvre.

Fédération des professionnels de l'intelligence économique (FéPIE)

Une cinquantaine de consultants, spécialisés dans le domaine de l'intelligence économique, ont créé en juillet 2005 la Fédération des professionnels de l'intelligence économique (FéPIE), véritable syndicat professionnel pour un secteur d'activité qui se met peu à peu en place en France, dont la présidence est assurée par l'amiral Pierre Lacoste, ancien directeur de la Direction générale de la Sécurité extérieure, (DGSE) entre 1982 et 1985[12]. Le but de cette Fédération est, d'une part, de promouvoir une éthique de l'intelligence économique, et, d'autre part, sensibiliser les entreprises françaises afin qu'elles acquièrent cette démarche méthodique enter protection et prospection de l'information. Ce qui intègre donc l'initiative de protéger ses propres savoir-faire et de connaître ceux des entreprises étrangères concurrentes. A terme, cela devrait conduire à la mise en place plusieurs collèges associés, l'un réunissant les chercheurs, formateurs et enseignants, un autre représentant les services publics ; un troisième réunissant les prestataires susceptibles

12) Le secrétariat général de la FéPIE est dirigé par Dominique Fonvielle.

d'être sollicités par des entreprises ; enfin, un Collège entreprises qui rassemble les entreprises clientes ou pratiquant l'intelligence économique.
A terme, il s'agit pour la FéPIE de constituer une organisation régionale avec la mise en place d'une labellisation des prestations d'Intelligence économique et d'un référentiel.
Les menaces qui pèsent sur la vie économique des PME/PMI sont prises très au sérieux par les pouvoirs publics. Au point que le ministère de l'Intérieur a lancé un programme d'intelligence économique territoriale sous la responsabilité directe des préfets. Par un volet défensif, il s'agit d'abord pour les pouvoirs publics, via les services de police et des Renseignements généraux, de sensibiliser les entreprises aux risques encourus à défaut de disposer de solides mesures de protection (notamment sur le plan informatique). Par un volet offensif, en prenant en compte le contexte d'extériorisation des activités entrepreneuriales, les préfectures de région sont invitées à mettre en place des réseaux d'échanges d'informations avec les PME/PMI. Le tout s'effectue en collaboration étroite avec l'Agence pour la diffusion de l'information technologique (ADIT) qui appuie l'action des préfets. Cette politique est initiée depuis 2004 à partir de neuf préfectures de région tests.

La mobilisation de la Préfecture Ile-de-France

La Préfecture élabore et met en œuvre le Schéma Régional d'Intelligence Economique en relation avec le Receveur Général des Finances, le Trésorier Payeur Général de la région Ile-de-France et en cas de nécessité le Haut Responsable pour l'Intelligence Economique. L'objectif est notamment la préparation d'un plan régional de sécurité économique au profit des PME/PMI identifiées comme les plus vulnérables dans des secteurs stratégiques, le renforcement de la place financière de Paris ou encore la promotion auprès des PME d'une démarche de conquêtes à l'étranger dans des prises de positions financières et stratégiques.

Orientations bibliographiques

AFDIE (Association française pour le développement de l'intelligence économique), « Modèle d'intelligence économique », préface d'Alain JUILLET, Economica, collection L'Intelligence Economique, 2004.

Philippe BAUMARD, « Stratégie et surveillance des environnements concurrentiels », Masson, coll. Stratégies et Systèmes d'Information, 2007.

Bernard BESSON et Jean-Claude POSSIN, « Du renseignement à l'intelligence économique. Détecter les menaces et les opportunités pour l'entreprise », Dunod, Paris, réédition 2001.

Bernard BESSON et Jean-Claude POSSIN, « L'intelligence des risques », IFIE (Institut Français de l'Intelligence Economique), coll. Pratique de l'IE, 2005.

Franck BOURNOIS et Pierre-Jacquelin ROMANI, « L'intelligence économique et stratégique dans les entreprises françaises », Economica et IHEDN, Paris, 2000.

Bernard CARAYON, « Intelligence économique, compétitivité et cohésion sociale », Rapport parlementaire au Premier ministre, La Documentation française, juin 2003.

CLUSIF (Club de la Sécurité de l'Information Français), « Panorama de la Cybercriminalité 2007 », www.clusif.asso.f

Eric DELBECQUE, « L'intelligence économique : Une nouvelle culture pour un nouveau monde », PUF, coll. Questions judiciaires, 2006.

Marcel DETIENNE et Jean-Pierre VERNANT, « Les ruses de l'intelligence : La mètis des Grecs », Champs Flammarion, 1993.

Sébastien DUBOIS, « L'intelligence économique : de la théorie à la pratique. Le cas Syngenta Agro », mémoire de Master IECS (Intelligence économique et communication stratégique), Université de Poitiers, 2005.

Grégoire DUPONT-TINGAUD, « Les aspects illicites de l'intelligence économique. Essai de définition des zones grises de l'infoguerre », mémoire

de Diplôme d'Université de 3e Cycle en Analyse des menaces criminelles contemporaines, Université Panthéon-Assas Paris II, année universitaire 2002/2003.

Jérôme DUPRÉ, « Renseignement et entreprises : Intelligence économique, espionnage industriel et sécurité juridique », Lavauzelle, coll. Renseignement et Guerre Secrète, 2002.

Philippe GUICHARDAZ, Pascal LOINTIER et Philippe ROSÉ, « L'infoguerre. Stratégies de contre-intelligence économique pour les entreprises », Dunod, Paris, 1999.

Christian HARBULOT, « Intelligence économique et guerre de l'information », Revue Mars, 1999.

Christian HARBULOT et Didier LUCAS (dir.), « La guerre cognitive : L'arme de la connaissance », Lavauzelle, coll. Renseignement et guerre secrète, Paris, 2002.

François-Bernard HUYGHE, « L'ennemi à l'ère numérique », PUF, coll. Défense et défis nouveaux, 2001.

François JULLIEN, « Le détour et l'accès : Stratégies du sens en Chine et en Grèce », Grasset, 1995.

Hervé LAROCHE et Jean-Pierre NIOCHE, « L'approche cognitive de la stratégie d'entreprise », Revue française de gestion, n°99, 1994.

Pascal LE PAUTREMAT, « Les nouveaux acteurs de la sécurité des entreprises », Raids, décembre 2002.

Frédéric LEROY, « Agressivité concurrentielle, taille de l'entreprise et performance », Actes de la dixième conférence de l'Association Internationale de Management Stratégique, Université Laval (Québec), 2001.

Didier LUCAS et Alain TIFFEREAU, « Guerre économique et information : Les stratégies de subversion », Ellipses, Paris, 2001.

Thibault du MANOIR DE JAYE, « Intelligence économique : utilisez toutes les ressources du droit », Editions d'Organisation, réédition 2003.

Daniel MARTIN et Frédéric-Paul MARTIN, « Cybercrime : menaces, vulnérabilités et ripostes », PUF, coll. Criminalité internationale, 2001.

Bruno MARTINET et Yves-Michel MARTI, « L'intelligence économique », Editions d'Organisation, réédition 2001.

Henri MARTRE (dir.), « Rapport du groupe Intelligence économique et stratégie des entreprises », Commissariat général du Plan, La Documentation française, février 1994.

Armand MATTELART, « La communication-monde. Histoire des idées et des stratégies », La Découverte, 1999.

Roger MONGEREAU, « Intelligence Economique, risques financiers et stratégies des entreprises », Conseil Economique et Social, 2006.

Jean-Claude MORAND, « RSS, Blogs : Un nouvel outil pour le management », M2 Editions, coll. Société, 2005.

Frédéric MOSER et Marc BORRY, « Intelligence économique et espionnage industriel : Côtés pile et face de l'information », Editions Luc Pire et L'Harmattan, 2002.

Joëlle NOAILLY, « L'espionnage industriel au cœur de la guerre mondiale du renseignement économique », mémoire de maîtrise de l'Université Lyon 2, année universitaire 1996/97.

Donald L. PIPKIN, « Sécurité des systèmes d'information. Protection globale des entreprises », Pearson Education France, 2000.

Daniel ROUACH, « La veille technologique et l'intelligence économique », PUF, coll. Que Sais-Je ?, réédition 2004.

Sources électroniques d'information

- Agence régionale de développement Paris Ile-de-France
  www.paris-region.com
- Agence régionale d'information stratégique et technologique de paris
  www.arist.ccip.fr
- Association nationale de la recherche technique
  www.anrt.asso.fr
- Centre d'alerte et de réaction aux attaques informatiques
  www.cert-ist.com
- Chambre Régionale de Commerce et d'Industrie de Paris Ile-de-France
  www.paris-iledefrance.cci.fr
- Club de la sécurité de l'information français
  www.clusif.asso.fr
- Club informatique des grandes entreprises françaises
  www.cigref.fr
- Commission nationale de l'informatique et des libertés
  www.cnil.fr
- Confédération générale des petites et moyennes entreprises
  www.cgpme75.fr
- Direction générale des douanes et droits indirects
  www.douane.gouv.fr
- Tracfin
  www.tracfin.minefi.gouv.fr
- Direction régionale de l'industrie, de la recherche et de l'environnement
  www.ile-de-france.drire.gouv.fr
- Fédération des professionnels de l'intelligence économique
  www.fepie.com
- Financement et accompagnement des PME
  www.oseo.fr
- Fondation d'entreprises dédiée à l'intelligence économique
  www.fondation-prometheus.org
- Information économique et sociale publique en Ile-de-France
  www.oeil-vif.org
- Observatoire de la sécurité des systèmes d'information et des réseaux
  www.ossir.org
- Portail d'intelligence économique de la CCI
  www.portail-intelligence.com
- Réseau de développement technologique d'Ile-de-France
  www.idf-tech.net
- Serveur thématique gouvernemental sur la sécurité des systèmes d'information
  www.ssi.gouv.fr
- Site de la mission du haut responsable en charge de l'intelligence économique
  www.intelligence-economique.gouv.fr

Coordonnées utiles :

Agefos PME Ile-de-France
11 rue Hélène –75849 Paris Cedex 17
Tél : 0826 301 311 – Fax : 01 40 08 16 09
Site Internet : www.agefos-pme-iledefrance.com

Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information (BEFTI) pour Paris et la Petite Couronne (92,93,94).
122 rue du Château des rentiers – 75013 Paris.
Tél : 01 55 75 26 19

CGPME Ile-de-France
10 Terrasse Bellini – 92806 Puteaux Cedex
Tél : 01 47 78 78 35 – Fax : 01 47 78 77 52
E-mail : contact@cgpme-idf.fr
Site Internet : www.cgpme-idf.fr

Conseil Régional d'Ile-de-France
Direction du développement économique et de l'emploi
Chargé de mission intelligence économique et stratégique
Tél : 01 53 85 67 14 – Fax : 01 53 85 60 49
Site Internet : www.iledefrance.fr

CRIE
Chargé de mission régional à l'intelligence économique
Recette Générale des Finances
Services de coordination à l'intelligence économique
94 rue réaumur – 75104 Paris Cedex 2.
Tél : 01 55 80 62 29 – Fax : 01 55 80 62 29

Etat-major de la région de gendarmerie d'Ile-de-France
Hôtel National des Invalides
BP 114 – 75326 Paris Cedex 07

Office Central de Lutte contre la Criminalité liées aux Technologies de l'Information et de la Communication (OCLCTIC).
101 Rue des 3 Fontanot – 92000 NANTERRE
Tél : 01 49 27 49 27 – Fax : 01 40 97 88 59
E-mail : oclctic@interieur.gouv.fr

Préfecture de la région Ile-de-France
29-33 rue Barbet-de-Jouy – 75700 Paris
Tél : 01 44 42 63 75 – Fax : 01 45 55 47 02
Site Internet : www.ile-de-france.pref.gouv.fr

Référents « intelligence économique »
de la gendarmerie départementale en Ile-de-France

UNITÉS	CORRESPONDANTS	TÉLÉPHONE
Groupement de gendarmerie départementale de la ville de Paris (Paris)	Colonel Jean-Pierre KOZLOWSKI	01 58 80 32 10
Groupement de gendarmerie départementale de Seine-et-Marne (Melun)	Chef d'escadron Philippe MARIE	01 64 71 71 11
Groupement de gendarmerie départementale des Yvelines (Versailles)	Lieutenant-colonel Jean-François ROYAL	01 39 67 50 02
Groupement de gendarmerie départementale de l'Essonne (Evry)	Lieutenant-colonel Patrick CHABROL	01 60 79 65 02
Groupement de gendarmerie départementale des Hauts-de-Seine (Nanterre)	Gendarme Patrick RETAILLEAI	01 40 97 44 55
Groupement de gendarmerie départementale de Seine-Saint-Denis (Bobigny)	Chef d'escadron Jean-François MORLON	01 48 96 30 02
Groupement de gendarmerie départementale du Val-de-Marne (Créteil)	Lieutenant Marc CULOS	01 49 80 27 33
Groupement de gendarmerie départementale du Val-d'Oise (Cergy)	Adjudant-chef Alain COLEAU	01 30 75 56 82

ERRATUM

« Guide rédigé par Pascal Le Pautremat
en coopération avec Patrice Lefort-Lavauzelle
Sous la direction de
La Direction des affaires économiques de la CGPME
et du Secrétariat général de la CGPME Ile-de-France »

Mention omise lors de l'édition 2008.

Imprimé en France
par l'imprimerie Vincent à Tours
Dépôt légal : 1er trimestre 2008

LE DIRIGEANT DE PME-PMI
L'INTELLIGENCE ÉCONOMIQUE

Les précautions à prendre au sein d'une PME-PMI

Alors que les tensions s'accroissent au niveau international,
il a semblé utile à la CGPME Ile-de-France de mettre à jour
ce guide dans le cadre du Schéma Régional
de Développement Économique , et face aux mutations économiques
vécues par les PME en Ile-de-France.

Avec nos partenaires, le Conseil Régional d'Ile-de-France
et Agefos PME Ile-de-France,
nous avons souhaité coller
au plus près du contexte régional.

Véritable guide opérationnel,
nous nous appuyons sur des cas fictifs
accompagnés de conseils pratiques, ainsi que
d'une importante bibliographie et d'une liste de sites spécialisés.